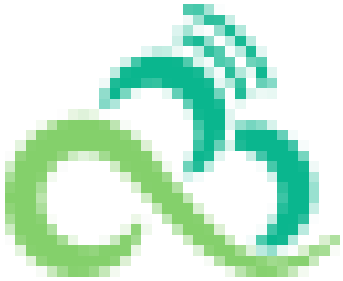
主机安全（CWP）

产品文档



文档目录

- 应急响应列表
- 安全管家列表
- 专家服务订单列表
- 安全管家月巡检报告下载
- 旗舰重保列表

入侵检测-反弹shell相关接口

- 删除反弹Shell事件
- 删除反弹Shell规则
- 获取反弹Shell列表
- 获取反弹Shell规则列表
- 导出反弹Shell事件

入侵检测-密码破解相关接口

- 删除暴力破解记录
- 获取爆破阻断模式
- 获取阻断地域
- 获取阻断按钮状态
- 获取阻断白名单列表
- 获取密码破解列表
- 获取爆破破解规则
- 导出密码破解记录
- 修改爆破阻断模式
- 设置阻断开关状态
- 修改暴力破解规则
- 不再提醒爆破阻断提示弹窗

入侵检测-异常登录相关接口

- 删除异地登录白名单规则
- 删除异地登录记录
- 获取登录审计列表
- 获取异地登录白名单合并后列表
- 获取异地登录白名单列表
- 查询常用登录地
- 导出异地登录记录

入侵检测-恶意请求相关接口

- 删除恶意请求记录
- 查询恶意请求白名单列表
- 获取恶意请求列表
- 导出下载恶意请求文件

入侵检测-文件查杀相关接口

- 创建网络攻击白名单
- 文件查杀检测
- 入侵管理-终止扫描任务
- 删除木马记录
- 删除网络攻击白名单
- 查询java内存马事件列表
- 获取木马列表
- 获取木马文件下载地址
- 查看恶意文件详情
- 风险预警提示
- 查询定时扫描配置
- 获取网络攻击白名单列表
- 查询木马扫描进度
- 获文件查杀概览信息
- 导出木马记录
- 定时扫描设置
- 编辑网络攻击白名单
- 恢复木马文件
- 隔离木马

- 根据策略名查询策略是否存在
- 基线影响主机列表导出
- 导出基线列表
- 已忽略基线检测项导出
- 忽略检测项影响主机列表导出
- 更新基线策略信息

安全运营相关接口

- 添加历史搜索记录
- 添加检索模板
- 删除检索模板
- 获取ES字段聚合结果
- 查询日志检索服务信息
- 获取索引列表
- 获取日志检索容量使用统计
- 导出ES查询文档列表
- 获取历史搜索记录
- 获取快速检索列表

新版基线管理相关接口

- 删除基线策略配置
- 删除基线规则
- 删除基线忽略规则
- 删除基线弱口令
- 获取基线检测详情记录
- 获取基线检测概览
- 获取基线下载列表
- 获取基线修复列表
- 获取基线检测主机列表
- 获取忽略规则主机列表
- 获取基线服务器风险TOP5
- 获取基线检测项的列表
- 获取忽略规则项列表
- 获取基线检测项信息
- 获取基线项检测结果列表
- 获取基线检测项TOP5
- 获取基线策略列表
- 获取基线分类列表
- 获取基线规则检测列表
- 获取基线忽略规则列表
- 获取基线规则列表
- 获取基线弱口令列表
- 获取全网热点漏洞
- 获取一键忽略受影响的检测项和主机信息
- 获取漏洞库列表
- 导出修复列表
- 导出基线主机检测
- 导出基线检测项
- 导出检测项结果列表
- 导出基线检测规则
- 导出弱口令配置列表
- 修复基线检测
- 修改或新增基线策略设置
- 修改或新增基线策略状态
- 修改或新增基线检测规则
- 修改或新增基线忽略规则
- 修改或新增弱口令
- 检测基线
- 停止基线检测

- 获取资源监控列表
- 查询资产管理计划任务列表
- 获取资产管理端口列表
- 获取资产管理进程列表
- 获取主机概况趋势
- 获取资产管理系统安装包列表
- 获取主机账号详情
- 获取账号列表
- 获取资产管理Web应用列表
- 获取资产管理Web应用插件列表
- 获取资产管理Web框架列表
- 获取Web站点详情
- 获取Web站点列表
- 查询资产管理Web服务列表
- 获取Web服务关联进程列表
- 获取组件统计列表
- 导出区域主机列表
- 获取帐号变更历史列表
- 查询批量导入机器信息
- 获取机器详情
- 查询机器操作系统列表
- 获取机器地域列表
- 获取区域主机列表
- 获取端口统计列表
- 获取进程统计列表
- 获取指定标签关联的服务器信息
- 获取所有主机标签
- 新增或编辑标签
- 导出资产管理内核模块列表
- 导出资产管理Web服务列表
- 修改主机备注信息
- 资产指纹启动扫描
- 同步资产扫描信息
- 关联机器标签列表

高级防御相关接口

- 添加网站防护服务器
- 删除网络攻击日志
- 删除防护网站
- 删除事件记录
- 网络攻击事件详情
- 按分页形式展示网络攻击检测事件列表
- 网络攻击日志详情
- 网络攻击日志列表
- 网络攻击数据统计
- 网络攻击top5数据列表
- 网络攻击趋势数据
- 获取网络攻击威胁类型列表
- 网页防篡改获取区域主机列表
- 查询网络攻击设置
- 防护目录列表
- 查询防护目录关联服务器
- 查询服务器关联目录详情
- 查询篡改事件列表
- 查询网页防篡改概览信息
- 查询网页防篡改防护统计
- 查询网站防篡改服务信息
- 导出网络攻击事件

产品简介
产品概述

最近更新时间: 2024-08-23 15:08:00

什么是主机安全

主机安全是一款针对多云主机的安全防护产品（支持尚航云_V1、非尚航云_V1主机接入），基于腾讯安全积累的海量威胁数据，利用机器学习为您提供黑客入侵检测和漏洞风险预警等安全防护服务，主要包括密码破解拦截、异常登录提醒、木马文件检测、高危漏洞检测等安全功能，解决当前服务器面临的主要网络安全风险，帮助企业构建服务器安全防护体系。

为什么需要主机安全

服务器一旦被黑客入侵，企业面临以下安全风险：

- **业务被中断**：数据库、文件被篡改或删除，导致服务无法访问，系统瘫痪。
- **数据被窃取**：黑客窃取企业数据后公开售卖，客户隐私数据被泄漏，造成企业品牌受损和客户流失。
- **被加密勒索**：黑客入侵服务器后通过植入不可逆的加密勒索软件对数据进行加密，对企业进行金钱勒索。
- **服务不稳定**：黑客在服务器中运行挖矿程序，并通过 DDoS 木马程序获取经济利益，消耗大量的系统资源，导致服务器不能提供正常服务。

使用主机安全可以有效预防以上问题，保障企业主机安全。

主机安全主要功能

文件查杀

网站后门木马又叫 Webshell，一般是黑客通过漏洞入侵网站后放置的 ASP、PHP、JSP 等动态脚本。黑客可以通过后门木马持续控制服务器，进行文件上传下载、执行命令等各种破坏行为，对网站安全危害极大。 基于机器学习的网站后门检测技术并依托尚航云_V1安全平台的全网恶意文件样本收集能力，主机安全可以实时准确的检测各类木马恶意文件，同时提供恶意文件检测和一键隔离等功能，保护您服务器的安全。

异常登录

基于常用登录源 IP、登录用户名、登录时间、登录地四个维度对服务器登录日志进行分析，以识别出登录流水中异常登录的行为，根据智能算法将异常登录记录标记为“可疑”或“高危”，并向您提供实时告警通知。

密码破解

您的云服务器可通过互联网登录，给了不法之徒进行暴力破解尝试入侵您云服务器的机会。尚航云_V1安全通过多维度多种手段检测云服务器是否被尝试暴力破解其密码。若检测有异常，会通过站内信或者短信等渠道对您进行告知。

恶意请求

主机安全通过对外界请求行为的实时监控及处理能力，实现对恶意请求行为的有效识别。若检测到恶意请求行为，主机安全系统会向您提供实时告警通知。

高危命令

基于尚航云_V1安全技术及多维度多种手段，对系统中命令实现实时监控，并且可通过配置规则对命令危险程度进行等级划分。若检测出高危命令，主机安全系统会向您提供实时告警通知。

本地提权

若出现以低权限进入系统，并通过某些手段提升权限，获取到高权限的事件，很有可能为黑客的攻击行为，该行为会危害到云服务器的安全。主机安全的本地提权功能可实时监控您服务器上的提权事件，并能对提权事件详情进行查看和处理，同时也支持白名单创建功能，用于设置被允许的提权行为。

反弹 Shell

反弹 Shell 功能是基于尚航云_V1安全技术及多维度多种手段，对服务器上的 Shell 反向连接行为进行识别记录，为您的云服务器提供反弹 Shell 行为的实时监控能力。

漏洞管理

主机安全对云服务器上存在的高危漏洞风险进行实时预警并提供修复方案，包括应急漏洞、Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞，帮助企业快速应对漏洞风险。

基线管理

尚航云_V1主机安全支持对基线检测项的定期检测和一键检测、支持对指定主机上的指定基线项进行检测、支持通过检测策略了解基线通过率及风险情况，同时可提供基线和检测项的风险等级和修复建议，同时提供尚航云_V1默认基线策略，有助于您更好的管理服务器中的基线安全。

高级防御

基于尚航云_V1安全技术，实时监控网络攻击行为，支持检测的威胁类型包括：Webshell 探测、Struts 漏洞利用、代码仓库拉取、代码注入攻击、命令注入攻击及机器批量控制利用等。

安全运营

根据《网络安全法》规定，日志存储时长不少于6个月，推荐每台服务器配置30GB存储容量以便采集和留存日志数据。日志分析提供木马、漏洞及网络安全事件等多维度的安全日志，支持语句检索和查询，并提供可视化报表、统计分析和导出功能，让您能够快速的排查和溯源主机上的安全事件，并提升运营效率。

产品优势

最近更新时间: 2024-08-23 15:08:00

主机安全与其他主机安全产品的优势比较如下表所示：

优势	腾讯主机安全	其他主机安全产品
黑客行为检测	基于云平台全网威胁数据源，实时检测黑客攻击行为 。	基于单机行为数据进行判断，检测能力弱，无法快速响应。
木马文件检测	后端集成电脑管家新一代 TAV 反病毒引擎及哈勃分析系统，极速响应未知风险。基于机器学习的 WebShell 检测引擎，有效对抗加密变形类恶意脚本。	可执行恶意文件的检测能力缺失，基于正则、字符逻辑匹配方式对 WebShell 进行检测，误报、漏报风险高。
免安装、维护	自动关联云平台服务器运维信息，购买云服务器即可使用相关信息。安全策略云端自动更新，无需人工维护各种安全检测脚本文件。	需要用户登录服务器手动安装，且需要一定安全技术能力的人进行安全策略配置。
集中运维	安全事件可在控制台统一管理，省去登录多台服务器的麻烦。主机资产集中管理，快速构建安全可视化运维平台。	需要登录到服务器上，对单个安全事件进行处理。
低资源占用	自研轻量级 Agent，绝大部分计算和防护在云端进行，对服务器的资源消耗占用低。	软件客户端内存占用高，普遍消耗在100M以上，业务峰期会影响服务器性能。

基本概念

最近更新时间: 2024-08-23 15:08:00

安全基线

安全基线（Security Base Line）指为了满足安全要求，相关系统和服务安全配置必须达到的一定标准和基本要求。通过对不同配置和策略的具体项目来评估产品是否达到安全基线，包括账号配置安全、口令配置安全、授权配置、日志配置、网络配置等。安全基线评估结果在一定程度上，反映了服务器的安全性。

木马病毒

木马病毒是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和 DDoS 攻击等特殊功能的后门程序。

WebShell

WebShell 就是以 ASP、PHP、JSP 或 CGI 等网页文件形式存在的一种命令执行环境，也称为一种网页后门。黑客在入侵了一个网站后，通常会将 ASP 或 PHP 后门文件与网站服务器 Web 目录下正常的网页文件混在一起，然后使用浏览器来访问 ASP 或者 PHP 后门，得到一个命令执行环境，以达到控制网站服务器的目的。

主机漏洞检测

主机漏洞检测（Host Vulnerability Detection）指基于主机 Agent 在主机内部发现漏洞的一种方式。将漏洞检测模块运行于主机内部，直接进行验证或者采集信息，来判断主机是否存在漏洞。

系统组件

组件（Component）或者通用组件，在主机安全层面主要泛指服务、应用对应的 Web 容器、软件等，例如 Nginx、Wordpress 等，而系统组件主要指非 Web 类的系统软件。

通用组件漏洞

通用组件漏洞又称为通用漏洞（Common Vulnerability），主要指通用组件而非业务自开发代码产生的漏洞，例如 WordPress 某个 SQL 注入、组件 Bash 的破壳漏洞等。

未授权访问

未授权访问（Unauthorized Access）是不满足安全基线导致的一类问题，主要指相关服务没有对服务的访问条件进行限制，例如设置密码、限制访问来源等，导致任何人都可以直接连接服务进行操作，从而产生安全问题。

异常登录

通过采集服务器上 RDP、SSH 登录日志，上报登录源 IP、登录用户名、登录时间、登录地等信息到云端进行风险评定，对非法登录进行实时告警通知。

隔离文件

隔离技术把存在恶意行为的木马、病毒文件进行隔离存储，避免恶意文件持续扩散。

快速入门

快速入门

最近更新时间: 2024-08-23 15:08:00

步骤1：安装主机安全

登录 主机安全控制台，进入安全概览页面，可查看云服务器是否已安装主机安全。

- 安装了主机安全开启专业版防护与旗舰版防护的云服务器，享有主机安全带来的全面多维度的系统安全保障。
- Windows 云服务器环境
- Linux 云服务器环境

Windows 云服务器环境

适配版本

目前支持的版本：

- Windows server 2012，2016，2019
- Windows server 2008 R2
- Windows server 2003（limited support）

主机安全客户端安装

服务器类型	服务器产品	服务器架构	所在网络	客户端下载安装
腾讯云	云服务器、轻量应用服务器、黑石服务器、边缘计算机器	x86	VPC 网络	wget http://u.yd.tencentyun.com/ydeyes_linux64.tar.gz -O ydeyes_linux64.tar.gz && tar -zxvf ydeyes_linux64.tar.gz && ./self_cloud_install_linux64.sh
腾讯云	云服务器	x86	基础网络	wget http://u.yd.qcloud.com/ydeyes_linux64.tar.gz -O ydeyes_linux64.tar.gz && tar -zxvf ydeyes_linux64.tar.gz && ./self_cloud_install_linux64.sh

服务器类型	服务器产品	服务器架构	所在网络	客户端下载安装
腾讯云	云服务器、轻量应用服务器、黑石服务器、边缘计算机器	arm	VPC 网络	wget http://u.yd.tencentyun.com/ydeyes/download/ydeyes_linux64_aarch64.tar.gz -O ydeyes_linux64_aarch64.tar.gz && tar -zxvf ydeyes_linux64_aarch64.tar.gz && ./self_cloud_install_linux64.sh
腾讯云	云服务器	arm	基础网络	wget http://u.yd.qcloud.com/ydeyes/download/ydeyes_linux64_aarch64.tar.gz -O ydeyes_linux64_aarch64.tar.gz && tar -zxvf ydeyes_linux64_aarch64.tar.gz && ./self_cloud_install_linux64.sh
非腾讯云	/	x86、arm	公网、专线	因存在命令有效期限制，请前往 主机列表 查看安装指引，进行客户端下载安装。

安装说明

执行命令，查看 YDService，YDLive进程是否有运行，有运行则安装成功。

`ps -ef | grep YD`

```
[root@VM_90_131_centos conf]# ps -ef|grep YD
root     16216 21992  0 14:33 pts/3    00:00:00 grep --color=auto YD
root     32707     1  0 11:23 ?        00:00:09 /usr/local/qcloud/YunJing/YDEyes/YDService
root     32724     1  0 11:23 ?        00:00:01 /usr/local/qcloud/YunJing/YDLive/YDLive
```

> **注意：**
>
> 若进程没有起来，可使用 root 用户手动执行命令，启动程序。命令为：
>
> `/usr/local/qcloud/YunJing/startYD.sh`

步骤2：操作主机安全

主机安全可对主机的安全信息进行实时处理和展示，支持对木马文件进行检测及隔离、漏洞检测、对可疑的登录行为进行检测识别及加白名单处理、支持对密码破解行为进行阻断设置、同时支持告警设置等操作，详情请参见 操作指南。

步骤3：故障排除

若主机遭遇入侵，可根据入侵类问题排查指南进行问题排查，恢复网站或系统的正常运行，详情请参见 Linux 入侵类问题排查思路 或 Windows 入侵类问题排查思路。

步骤4：卸载主机安全

若您不再需要主机安全防护，可将其卸载，主机安全共有控制台卸载与系统卸载两种方式，下面将为您详细介绍：

控制台中卸载

1. 登录 主机安全控制台，在左侧导航栏，选择**资产管理** > **主机列表**，查看自己的云服务器是否已安装主机安全。

   在服务器列表中，可选择需要卸载主机安全的服务器，在右侧操作栏，单击**卸载**即可。

进入系统卸载

- **Windows 系统**：依照路径 `C:\Program Files\QCloud\YunJing\uninst.exe` ，找到 `uninst.exe` 文件，双击即可卸载。
- **Linux 系统**：输入命令： `if [ -w &#39;/usr&#39; ]; then /usr/local/qcloud/YunJing/uninst.sh ; else /var/lib/qcloud/YunJing/uninst.sh ; fi` 即可卸载。

常见问题

安装时遇到防火墙拦截要如何处理？

建议防火墙策略放通主机安全后台服务器访问地址：

- VPC 网络域名： s.yd.cloud.sunhongs.com、l.yd.cloud.sunhongs.com、u.yd.cloud.sunhongs.com
- VPC 网络 IP： 169.254.0.55
- 基础网络域名： s.yd.qcloud.com、u.yd.qcloud.com、l.yd.qcloud.com
- 基础网络 IP： 10.148.188.202、10.148.188.201、11.177.125.116、11.177.124.86、11.149.252.57、11.149.252.62、11.149.252.51
- 非尚航云_V1公网域名： sp.yd.qcloud.com、up.yd.qcloud.com、lp.yd.qcloud.com
- 非尚航云_V1公网 IP： 120.232.65.223、157.148.45.20、183.2.143.163
- 端口： 5574、8080、80、9080（公网还需放过443端口）

若不使用默认 DNS，要如何设置？

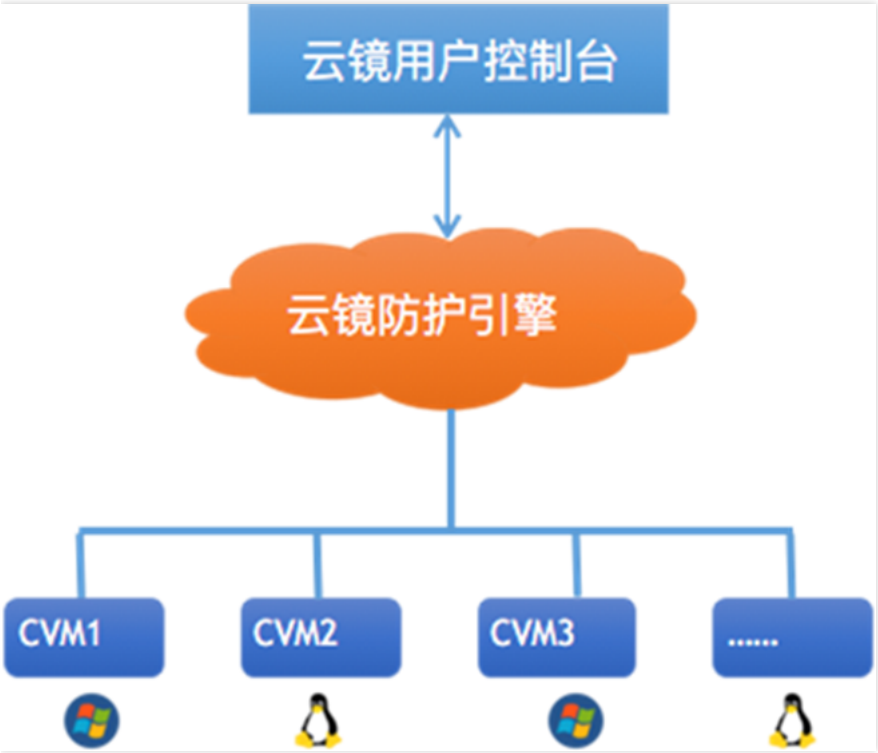
若您不使用默认 DNS，则需要将 cloud.sunhongs.com 和 yd.qcloud.com 根域的所有解析转发至默认 DNS。

产品架构

产品架构

最近更新时间: 2024-08-23 15:08:00

下图是云镜的产品架构示意图：



云镜Agent

Agent是一个常驻在云主机操作系统中的轻量化进程，部署在需要保护的云主机上，主要功能是根据用户配置的安全策略上报服务器上存在的安全风险数据和新增的安全事件数据，同时响应用户和云镜云端防护中心的指令，实现对云主机上的安全威胁清除和恶意攻击拦截。

云镜防护引擎

基于腾讯的大数据处理能力，云端防护中心接收全网Agent上报云主机安全事件和威胁数据，通过云端的多个威胁识别模型，对每一条上报的安全事件进行分析，根据分析结果给Agent下发相关拦截和处理指令，云端防护中心是云镜的中枢神经系统，相关安全威胁的识别算法依赖于腾讯云安全团队的运营和智能调优，云端防护中心同时保存用户自己创建的相关安全策略配置，满足用户个性化的安全防护需求。

用户操作控制台

提供给用户使用的网页版本控制台，主要功能包括云主机资产管理、安全威胁数据处理、安全策略配置、安全报表查看等供用户操作和查看的功能。

故障处理
Linux入侵类问题排查思路

最近更新时间: 2024-08-23 15:08:00

本文档将指导您如何排查 Linux 入侵类问题并提供被入侵后的安全优化建议。

> **说明：**
>
> 若已明确入侵事件属于挖矿或木马，请按 挖矿木马自助清理手册 进行处置。

深入分析，查找入侵原因

一、检查隐藏账户及弱口令

1. 检查服务器系统及应用账户是否存在**弱口令**：
   - 检查说明：检查管理员账户、数据库账户、MySQL 账户、tomcat 账户、网站后台管理员账户等密码设置是否较为简单，简单的密码很容易被黑客破解。
   - 解决方法：以管理员权限登录系统或应用程序后台，修改为复杂的密码。
   - 风险性：高。
2. 使用 `last` 命令查看下服务器近期登录的账户记录，确认是否有可疑 IP 登录过机器：
   - 检查说明：攻击者或者恶意软件往往会往系统中注入隐藏的系统账户实施提权或其他破坏性的攻击。
   - 解决方法：检查发现有可疑用户时，可使用命令 `usermod -L 用户名` 禁用用户或者使用命令 `userdel -r 用户名` 删除用户。
   - 风险性：高。
3. 通过 `less /var/log/secure|grep &#39;Accepted&#39;` 命令，查看是否有可疑 IP 成功登录机器：
   - 检查说明：攻击者或者恶意软件往往会往系统中注入隐藏的系统账户实施提权或其他破坏性的攻击。
   - 解决方法：使用命令 `usermod -L 用户名` 禁用用户或者使用命令 `userdel -r 用户名` 删除用户。
   - 风险性：高。
4. 检查系统是否采用**默认管理端口**：
   - 检查系统所用的管理端口（SSH、FTP、MySQL、Redis 等）是否为默认端口，这些默认端口往往被容易自动化的工具进行暴破成功。
   - 解决方法：

     a.在服务器内编辑 `/etc/ssh/sshd_config` 文件中的 Port 22，将22修改为非默认端口，修改之后需要重启 ssh 服务。

> **注意：**
>
> 当对端口进行修改时，需同时在云服务器控制台上修改对应主机的安全组配置，在其入站规则中，放行对应端口，详情请参见 添加安全组规则。

b.运行/etc/init.d/sshd restart（CentOS）或 /etc/init.d/ssh restart（Debian / Ubuntu）命令重启使配置生效。

c.修改 FTP、MySQL、Redis 等的程序配置文件的默认监听端口21、3306、6379为其他端口。

d.限制远程登录的 IP，编辑/etc/hosts.deny 、/etc/hosts.allow两个文件来限制 IP。

- 风险性：高。

5. 检查/etc/passwd文件，看是否有非授权账户登录：

- 检查说明：攻击者或者恶意软件往往会往系统中注入隐藏的系统账户实施提权或其他破坏性的攻击。
- 解决方法：使用命令 `usermod -L 用户名` 禁用用户或者使用命令 `userdel -r 用户名` 删除用户。
- 风险性：中。

二、检查恶意进程及非法端口

1. 运行 `netstat -antp` ，查看服务器是否有未被授权的端口被监听，查看下对应的 pid。

- 检查服务器是否存在恶意进程，恶意进程往往会开启监听端口，与外部控制机器进行连接。
- 解决方法：若发现有非授权进程，运行 `ls -l /proc/$PID/exe` 或 `file /proc/$PID/exe` （ $PID 为对应的 pid 号），查看下 pid 所对应的进程文件路径。

如果为恶意进程，删除对应的文件即可。

- 风险性：高。

2. 使用 `ps -ef` 和 `top` 命令查看是否有异常进程

- 检查说明：运行以上命令，当发现有名称不断变化的非授权进程占用大量系统 CPU 或内存资源时，则可能为恶意程序。
- 解决方法：确认该进程为恶意进程后，可以使用 `kill -9 进程名` 命令结束进程，或使用防火墙限制进程外联。
- 风险性：高。

三、检查恶意程序和可疑启动项

1. 使用 `chkconfig --list` 和 `cat /etc/rc.local` 命令，查看开机启动项中是否有异常的启动服务。

- 检查说明：恶意程序往往会添加在系统的启动项，在用户关机重启后再次运行。
- 解决方法：如发现有恶意进程，可使用 `chkconfig 服务名 off` 命令关闭，同时检查 `/etc/rc.local` 中是否有异常项目，如有请注释掉。
- 风险性：高。

2. 进入 cron 文件目录，查看是否存在非法定时任务脚本。

- 检查说明：查看 `/etc/crontab` ， `/etc/cron.d` ， `/etc/cron.daily` ， `cron.hourly/` ， `cron.monthly` ， `cron.weekly/` 是否存在可疑脚本或程序。
- 解决方法：如发现有不认识的计划任务，可定位脚本确认是否正常业务脚本，如果非正常业务脚本，可直接注释掉任务内容或删除脚本。
- 风险性：高。

四、检查第三方软件漏洞

1. 如果您服务器内有运行 Web、数据库等应用服务，请您限制应用程序账户对文件系统的写权限，同时尽量使用非 root 账户运行。

- 检查说明：使用非 root 账户运行，可以保障在应用程序被攻陷后，攻击者无法立即远程控制服务器，减少攻击损失。
- 解决方法：进入 web 服务根目录或数据库配置目录。

运行 `chown -R apache:apache /var/www/xxxx` 、 `chmod -R 750 file1.txt` 命令配置网站访问权限。

- 风险性：中。
- 具体参考下方网站目录文件权限示例。

2. 升级修复应用程序漏洞

   - 检查说明：机器被入侵，部分原因是系统使用的应用程序软件版本较老，存在较多的漏洞而没有修复，导致可以被入侵利用。
   - 解决方法：比较典型的漏洞例如 ImageMagick、openssl、glibc 等，用户可以根据尚航云_V1已发布的安全通告指导或通过 apt-get/yum 等方式进行直接升级修复。
   - 风险性：高。

网站目录文件权限的参考示例如下：场景：** 假设 HTTP 服务器运行的用户和用户组是 www，网站用户为 centos，网站根目录是 `/home/centos/web` 。 **方法/步骤：**

1. 我们首先设定网站目录和文件的所有者和所有组为 centos，www，如下命令：

```
chown -R centos:www /home/centos/web
```

2. 设置网站目录权限为750，750是 centos 用户对目录拥有读写执行的权限，设置后，centos 用户可以在任何目录下创建文件，用户组有有读执行权限，这样才能进入目录，其它用户没有任何权限。

```
find -type d -exec chmod 750 {} \;
```

3. 设置网站文件权限为640，640指只有 centos 用户对网站文件有更改的权限，HTTP 服务器只有读取文件的权限，无法更改文件，其它用户无任何权限。

```
find -not -type d -exec chmod 640 {} \;
```

4. 针对个别目录设置可写权限。例如，网站的一些缓存目录就需要给 HTTP 服务有写入权限、discuz x2 的 `/data/` 目录就必须要写入权限。

```
find data -type d -exec chmod 770 {} \;
```

被入侵后的安全优化建议

- 推荐使用 SSH 密钥进行登录，减少暴力破解的风险。
- 在服务器内编辑 `/etc/ssh/sshd_config` 文件中的 Port 22，将 22 修改为其他非默认端口，修改之后重启 SSH 服务。可使用如下命令重启：

```
/etc/init.d/sshd restart（CentOS）或 /etc/init.d/ssh restart（Debian/Ubuntu）
```

> **注意：**
>
> 当修改端口时，需同时在云服务器控制台上修改对应主机安全组配置，在其入站规则中放行对应端口，详情请参见 添加安全组规则。

- 如果必须使用 SSH 密码进行管理，选择一个好密码。
- 无论应用程序管理后台（网站、中间件、tomcat 等）、远程 SSH、远程桌面、数据库，都建议设置复杂且不一样的密码。
- 下面是一些好密码的实例（可以使用空格）： `1qtwo-threeMiles3c45jia`` caser, lanqiu streets`
- 下面是一些弱口令的示例，可能是您在公开的工作中常用的词或者是您生活中常用的词： 公司名+日期（coca-cola2016xxxx） 常用口语（Iamagoodboy）
- 使用以下命令检查主机有哪些端口开放，关闭非业务端口。

```
netstat -antp
```

- 通过尚航云_V1-安全组防火墙限制仅允许制定 IP 访问管理或通过编辑 `/etc/hosts.deny` 、 `/etc/hosts.allow` 两个文件来限制 IP。
- 应用程序尽量不使用 **root** 权限。 例如 Apache、Redis、MySQL、Nginx 等程序，尽量不要以 root 权限的方式运行。
- 修复系统提权漏洞与运行在 root 权限下的**程序漏洞**，以免恶意软件通过漏洞提权获得 root 权限传播后门。

- 及时更新系统或所用应用程序的版本，如 Struts2、Nginx，ImageMagick、Java 等。
- 关闭应用程序的远程管理功能，如 Redis、NTP 等，如果无远程管理需要，可关闭对外监听端口或配置。
- 定期**备份**云服务器业务数据。
- 对重要的业务数据进行异地备份或云备份，避免主机被入侵后无法恢复。
- 除了您的 home，root 目录外，您还应当备份 /etc 和可用于取证的 /var/log 目录。
- 安装尚航云_V1**主机安全 Agent**，在发生攻击后，可以了解自身风险情况。

> **说明：**
>
> 如果以上步骤均不能排查出来问题，建议您联系运维人员进行处理。

Windows入侵类问题排查思路

最近更新时间: 2024-08-23 15:08:00

本文档将指导您如何排查 Windows 入侵类问题。

深入分析，查找入侵原因

一. 检查帐户和弱口令

1. 查看服务器已有系统或应用帐户是否存在弱口令。
   - 检查说明：主要检查系统管理员帐户、网站后台帐户、数据库帐户以及其他应用程序（FTP、Tomcat、phpMyAdmin 等）帐户是否存在弱口令。

> **说明：**
>
> 帐户密码建议设置为大写、小写、特殊字符、数字组成的12 - 16位的复杂密码 ，也可使用密码生成器自动生成复杂密码

- 检查方法：根据实际情况自行确认。
- 风险性：**高。**

2. 查看下服务器内是否有非系统和用户本身创建的账户。
   - 检查说明：一般黑客创建的异常账户账户名会在本地用户组显示出来。
   - 检查方法：打开 cmd 窗口，输入 `lusrmgr.msc` 命令，查看是否有新增的账户，如有管理员群组的（Administrators）里的新增账户，请立即禁用或删除掉。
   - 风险性：**高。**

3. 检查是否存在隐藏账户名。
   - 检查说明：黑客为了逃避检查，往往会在您服务器内创建隐藏账户，隐藏账户在本地用户内是查看不到的。
   - 检查方法（您也可以通过下载 LP_Check 安全工具检查是否有隐藏账户）：

     a.在桌面打开运行（可使用快捷键 Win + R），输入 regedit，即可打开注册表编辑器。

     b.选择 HKEY_LOCAL_MACHINE/SAM/SAM，默认无法查看该选项内容，右键菜单选择权限，打开权限管理窗口。

     c.选择当前用户（一般为 administrator），将权限勾选为完全控制，然后确定，关闭注册表编辑器。

     d.再次打开注册表编辑器，即可选择 HKEY_LOCAL_MACHINE/SAM/SAM/Domains/Account/Users。

     e.在 Names 项下可以看到实例所有用户名，如出现本地账户中没有的账户，即为隐藏账户，在确认为非系统用户的前提下，可删除此用户。
   - 风险性：**高。**

二. 检查恶意进程和端口

1. 检查是否存在恶意进程在系统后台运行。
   - 检查说明：攻击者在入侵系统后，往往会运行恶意进程与外部进行通信，通过分析外联的进程，即可以找出入侵的控制进程。
   - 检查方法：

     a.登录服务器，选择**开始** > **运行。**

     b.输入 `cmd` ，然后输入 `netstat –nao` 查看下服务器是否有未被授权的端口被监听。

c.打开任务管理器，检查对应的 PID 进程号所对应的进程是否为正常进程，例如通过 PID 号查看下运行文件的路径，删除对应路径文件，您也可以通过微软官方提供的 Process Explorer 工具进行排查。

- 风险性：**高。**

三. 检查恶意程序及启动项

1. 检查服务器内部是否有异常的启动项。

- 检查说明：攻击者在入侵系统后，往往会把恶意程序放到启动项中开机执行。
- 检查方法：

  a.登录服务器，选择**开始** > **所有程序**>**启动。**

  b.默认情况下此目录在是一个空目录，确认是否有非业务程序在该目录下。

  c.选择**开始** > **运行**，输入 `msconfig` ，查看是否存在命名异常的启动项目，若存在则取消勾选命名异常的启动项目，并到命令中显示的路径删除文件。

  d.选择**开始** > **运行**，输入 `regedit` ，打开注册表，查看开机启动项是否正常，特别注意如下三个注册表项：HKEY_CURRENT_USER\software\micorsoft\windows\currentversion\run HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce 检查注册表右侧是否有启动异常的项目，如有请删除，并建议安装杀毒软件进行病毒查杀，清除残留病毒或木马。

- 风险性：**高。**

2. 查看正在连接的会话。

- 检查说明：检查服务器与网络上的其它服务器之间的会话或计划任务。
- 检查方法：

  a.登录服务器，选择**开始** > **运行。**

  b.输入 `cmd` ，然后输入 `netstat -ano` ，检查服务器与网络上的其它服务器之间的会话，并确认是否为正常连接。输入 schtasks，检查服务器中的计划任务，并确认是否为正常的计划任务。

- 风险性：**中。**

四. 检查第三方软件漏洞

1. 如果您服务器内有运行对外应用软件（WWW、FTP 等），请您对软件进行配置，**限制应用程序的权限，禁止目录浏览或文件写权限。**

2. 开通尚航云_V1 Web 应用防火墙 防护，查看 Web 应用防护攻击日志。

常见问题

如何恢复被入侵后的网站或系统？

系统确认被入侵后，往往系统文件会被更改和替换，此时系统已经变得不可信，最好的方法就是重新安装系统，同时给新系统安装所有补丁。

如何防止网站或系统被再次入侵？

1. 改变所有系统账户的密码为 **复杂密码**（至少与入侵前不一致）。

2. **修改默认远程桌面端口**，操作如下：

   i. 选择**开始** > **运行**，然后输入 `regedit` 。

ii. 打开注册表，进入如下路径： HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp

iii. KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Tenninal Server\WinStations\RDP-Tcp

iv. 修改下右侧的 PortNamber 值。

3. 配置尚航云_V1安全组防火墙只允许 **指定 IP 才能访问远程桌面端口。**

4. **定期备份**重要业务数据和文件。

5. **定期更新**操作系统及应用程序组件版本（如 FTP、Struts2 等），防止被漏洞利用。

6. 安装**尚航云_V1主机安全 Agent** 和防病毒软件进行定期体检和扫描。

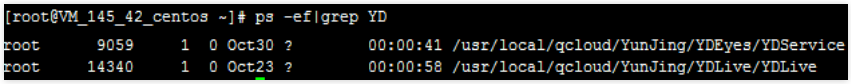
Linux 客户端离线排查

最近更新时间: 2024-08-23 15:08:00

本文档将指导您进行 Linux 客户端离线排查，包括客户端进程未启动排查及网络故障排查。

客户端进程未启动排查

1. 请查询主机安全进程是否存在。输入： `ps -ef|grep YD` 。



正常状态下，主机安全存在两个进程，如下图所示：

- 如果进程不存在，可能存在以下情况：
- 服务器未安装主机安全或者客户端已被卸载，请根据 快速入门 安装指引，进行客户端安装。
- 客户端可能出现异常冲突或者崩溃，导致进程没有启动。

2. 若服务器已安装主机安全或者客户端，可采用以下方法排查客户端进程未启动原因：

- 可查看客户端日志，存放路径： `/usr/local/qcloud/YunJing/log` 。
- 可执行命令： `sh /usr/local/qcloud/YunJing/startYD.sh` 启动主机安全服务。

网络故障排查

如果进程存在，但主机安全不在线，大部分原因是网络不通，请按照以下操作进行排查：

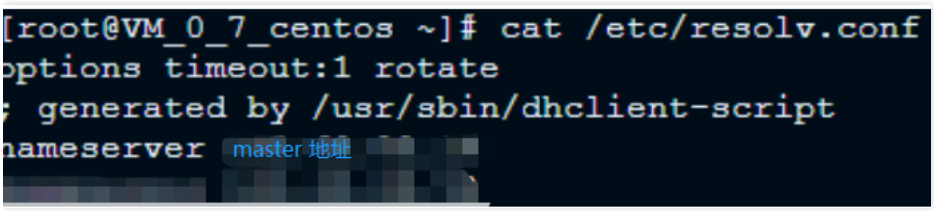
1. 如果无法访问主机安全域名，可以尝试修改 DNS。可以通过执行如下命令行，排查主机安全域名是否可以访问：
   - VPC 网络和黑石服务器环境： `telnet s.yd.cloud.sunhongs.com 5574` 。

     正常情况下：返回如下图所示结果。

如果无法访问：

a. 可以尝试修改`dns nameserver`字段：`vim /etc/resolv.conf``nameserver master地址`

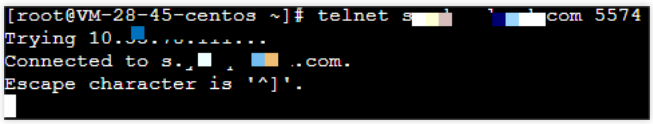
b. 修改完成后，重新执行`telnet s.yd.cloud.sunhongs.com 5574`检测能否连通。



c. 如果可以连通，等待几分钟后（时间长短根据网络情况而定），控制台将能看到对应服务器重新上线。

- 基础网络环境（非 VPC 上的服务器）：`telnet s.yd.cloud.sunhongs.com 5574`。

  正常情况下：返回如下图所示结果。



  如果无法访问：

  a. 可以尝试修改`dns nameserver`字段：`vim /etc/resolv.conf`，先把原有的`nameserver`字段注释，再新增 `nameserver`字段，具体的 nameserver ip 相关内容，请参见[内网服务](/document/product/292128/5225)。

  b. 修改完成后，重新执行`telnet s.yd.cloud.sunhongs.com 5574`检测能否连通。

  c. 如果可以连通，等待几分钟后（时间长短根据网络情况而定），控制台将能看到对应服务器重新上线。

2. 防火墙策略限制，需要在 Linux 客户端开放 TCP 端口：5574、8080、80、9080。

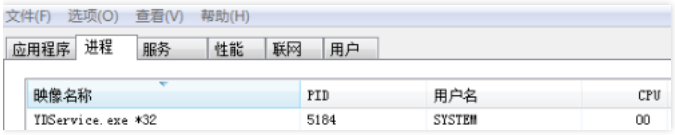
3. 如果主机安全进程存在，且不是由于网络原因导致的客户端离线，请打包客户端日志（日志路径：`/usr/local/qcloud/YunJing/log`）并 提交工单 进行反馈。

Windows 客户端离线排查

最近更新时间: 2024-08-23 15:08:00

客户端进程未启动排查

请查询主机安全进程是否存在。 打开 Windows 任务管理器，查找名为 YDService.exe 的进程是否存在。



1. 如果进程不存在，可能存在以下情况：

   - 服务器未安装主机安全或者客户端已被卸载，请根据 快速入门 安装指引，进行客户端安装。
   - 客户端可能出现异常冲突或者崩溃，导致进程没有启动。

2. 排查方法：

   - 可查看客户端日志，存放路径： C:\Program Files\QCloud\YunJing\log 。
   - 可执行命令： sc start ydservice 手动运行客户端。

网络故障排查

如果进程存在，但主机安全客户端不在线，大部分原因是网络不通，请按照以下操作进行排查：

1. 检查 DNS 是否被修改，可以通过执行如下命令行进行排查，只要其中一个返回正常结果，则表示 DNS 无问题：

   - 基础网络下载地址（非 VPC 服务器）： telnet s.yd.cloud.sunhongs.com 5574 。
   - VPC 和黑石服务器下载： telnet s.yd.cloud.sunhongs.com 5574。

2. 防火墙阻拦导致故障，需要开放5574、8080、80、9080端口。

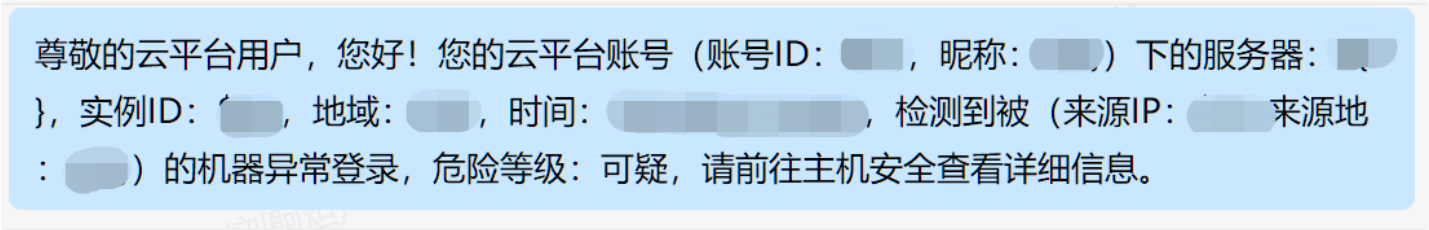
3. 如果主机安全进程存在，且不是由于网络原因导致的客户端离线，请打包客户端日志（日志路径： C:\Program Files\QCloud\YunJing\log ）提交工单 进行反馈。

异常登录的消息提醒

最近更新时间: 2024-08-23 15:08:00

现象描述

用户接收到尚航云_V1发送的服务器被异常登录的消息提醒，如下以短信消息为例：



可能原因

当您尚航云_V1账号下的服务器有登录行为时，尚航云_V1主机安全若发现本次登录没有命中登录白名单，会根据智能算法将该登录记录标记为"可疑"或"高危"，并触发实时告警提醒。

> 说明：
>
> - 默认仅告警危险等级为"高危"的异常登录事件，可通过**设置中心**> **告警设置**勾选设置。
> - 异常登录危险等级是依托算法对服务器过往登录情况综合判定。

处理步骤

在收到的异常登录告警提醒后，请您按照下列步骤进行确认：

1. 请确认本次登录行为是否为合法登录。
   - 是，请将该登录记录加入白名单，后续该登录行为再次发生，不再产生告警。

- 否，请执行步骤2。

2. 确定为非法登录，初步判断您服务器告警的异常登录事件，是由于不常使用的用户被破解，建议您立即修改登录密码以及服务器上保存过的相关登录凭证。建议参考 Linux 入侵类问题排查思路 和 Windows 入侵类问题排查思路对服务器进行常规排查。

加固方法

后续您可以通过如下加固方法，以提高服务器安全性：

- 服务器设置大写、小写、特殊字符、数字组成的12-16位的复杂密码。
- 修改云服务器 Linux 系统默认远程登录端口，如下所示： 修改文件：/etc/ssh/sshd_config

```
Port 22 #在第三行或第四行，如果前面有井号，请删除，修改为65534以下即可
```

可在远程连接中用 vi 命令，或 sftp 下载到本地修改，修改后使用以下命令重启 ssh 服务。

```
/etc/init.d/sshd restart #centos系统，重启ssh服务命令
/etc/init.d/ssh restart #debian/ubuntu系统，重启 ssh 服务命令
```

尚航云_V1平台有安全组功能，建议您仅放行需要的业务协议和端口，不建议放行所有协议所有端口 ，详情请参考 创建安全组。

配置云服务器系统防火墙，建议开启云防火墙 。

确保云服务器已安装的防护软件 主机安全客户端进程 处于正常运行状态，并开启实时告警，有异常登录时，及时反馈到您。

及时修复云服务器系统组件与 Web 组件存在的安全漏洞。

> **说明：**
>
> 做好如上云服务器系统安全防护，虽可有效降低安全风险，但也无法保证绝对安全，建议定期做好云服务器系统的安全巡检及数据备份，以防突发情况导致数据丢失、或业务不可用。 在安全加固的同时，也强烈建议您通过制作系统镜像、创建数据快照、自动定期快照

常见问题

- **是否可以关闭异常登录检测？**

不可以关闭异常登录检测。

如果您不想接收异常登录的告警通知，您可以尽量配全登录白名单，或者关闭异常登录告警。

配全登录白名单：在 异常登录页，选择**白名单管理** > **添加白名单**，将常用登录来源 IP 添加为白名单。

关闭异常登录告警：在 设置中心页面，将告警状态设为关闭，或取消勾选告警项“高危”或“可疑”即可。

常见问题
购买相关

最近更新时间: 2024-08-23 15:08:00

如何购买主机安全专业版与旗舰版？

可以进入 主机安全购买页 进行升级。

如何关闭主机安全专业防护或旗舰防护服务？

进入 授权管理页面，查看授权详情，可对已绑定授权的主机进行如下操作：

- 专业版-按量计费：您可执行解绑或者关闭专业版操作。解绑：每台主机每月仅有一次解绑机会；关闭专业版：关闭后授权数将-1（若仅有1个授权的情况，关闭专业版后则直接销毁该授权订单）。

- 专业版-包年包月和旗舰版-包年包月：您可执行解绑操作。解绑：每台主机每月仅有一次解绑机会。

注意：

- 云服务器到期或手动销毁后，主机安全专业版/旗舰版防护授权将自动解绑，空闲出来的授权可以去绑定其他主机。
- 关闭主机安全专业防护与旗舰防护服务后，将不再提供对该主机的高危漏洞监控预警服务。
- 主机安全是否扣费以实际购买的授权数为准，与授权是否绑定了主机、主机是否开机无关。

新购云服务器，为何会自动生成主机安全专业防护的子订单？

若在主机安全控制台的 授权管理 中，打开自动升级防护的开关，新增加的云服务器都会自动升级为专业防护版，订单中会自动生成购买主机安全专业防护的子订单。

主机安全产品是否与其他安全产品冲突？

主机安全与其他安全产品并不冲突，属于不同的防护维度，通过在不同的层面上提供安全能力，保障用户安全。

如何卸载云服务器主机安全客户端?

登录 主机安全控制台，在左侧导航栏选择**资产管理** > **主机列表**，在服务器列表，找到需要卸载的云服务器单击**卸载**，或打开安装目录，通过目录中的卸载程序进行卸载。

功能相关

最近更新时间: 2024-08-23 15:08:00

病毒库及漏洞库更新周期是多久？

病毒库：每天00:00更新。 漏洞库：不定时更新。

为什么 Jar 包类的漏洞多次扫描时，每次检测结果可能不一致？

Jar 包类漏洞，例如 struts2 漏洞的检测依赖 Jar 包运行态是否加载，未运行服务时是不能检测到漏洞的，运行服务时 Webserver 对于Jar 包的加载分为动态加载和静态加载。在动态加载模式下，struts2 漏洞只有在 Jar 包运行时才能被检测出来，所以每个时段检测结果存在差异。建议您针对高危 Jar 包漏洞进行多次检测，提升检测结果的准确度。

主机安全扫描频率是多少？

- 主机安全基础版：提供一次性检测。
- 主机安全专业版：可自定义周期。
- 主机安全旗舰版：可自定义周期。

如何对木马文件进行处理？

在 文件查杀 页面，可对木马文件进行如下处理：

- 删除：单击复制木马文件路径，定位木马并手动删除该文件。

- 信任：您可执行信任操作，后续主机安全将不再对该机器的该文件进行检测。
- 隔离：当前尚不支持拦截木马，仅支持事中或事后检测并告警，但可对该文件执行隔离操作，防止该文件再次被启动。

概览页安全评分机制是怎样的？

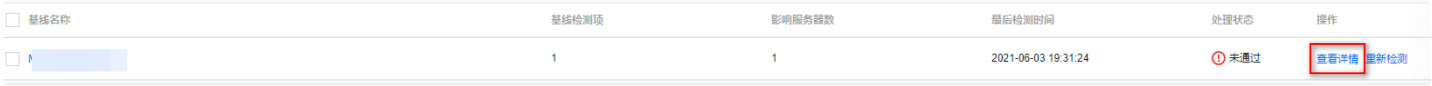
概览页安全评分机制，请参见 安全概览 文档。

安全基线在产品设置过后，多久可以生效？

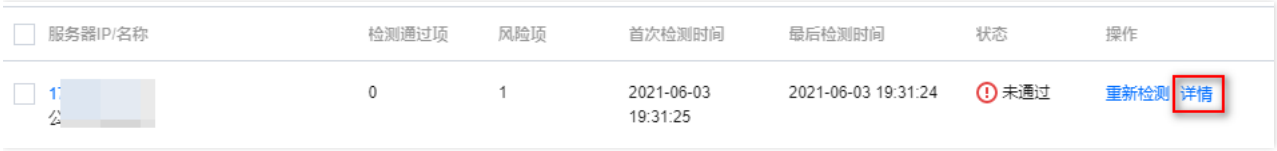
安全基线在产品设置后，即时生效。

主机安全基线检测“未通过”怎么处理？

1. 进入 安全基线 页面，选择未通过的检测项，单击操作列下的查看详情，进入该检测项的详情页面。



2. 在详情页面，选择所需服务器 IP，单击详情，进入检测详情页面。



3. 在检测详情页面，将鼠标 放置处，即可查看该基线的对应处理建议。

主机安全发现漏洞木马等攻击是否会进行通知？

会，若主机安全发现木马、应急漏洞或者其他攻击的行为，会通过站内信、短信、邮件或企业微信方式的方式进行告警通知，具体方式您可以在 消息中心 进行设置。

入侵相关

最近更新时间: 2024-08-23 15:08:00

入侵常见问题

云服务器被入侵有哪些危害？

- 业务被中断：数据库、文件被篡改或删除，导致服务无法访问，系统瘫痪。
- 数据被窃取：黑客窃取企业数据后公开售卖，客户隐私数据被泄漏，导致企业品牌受损、用户流失。
- 被加密勒索：黑客入侵云服务器后通过植入不可逆的加密勒索软件对数据进行加密，对企业进行金钱勒索。
- 服务不稳定：黑客在云服务器中运行挖矿程序、DDoS 木马程序，消耗大量系统资源，导致云服务器不能提供正常服务。

如何降低云服务器被入侵概率？

- 及时修复高危漏洞及基线相关问题。
- 设置强密码，避免暴破攻击。
- 定期巡检账号、权限、端口并及时处理 主机安全控制台 的告警信息。

云服务器被入侵后要如何防护？

防范措施建议如下：

- 云服务器密码设置为大写、小写、特殊字符、数字组成的12 - 16位的复杂密码 ，也可使用密码生成器自动生成复杂密码。
- 删除云服务器上设置的不需要的用户，且对于不需要登录的用户，请将其权限设置为禁止登录。
- 修改远程登录服务的默认端口号并禁止超级管理员用户登录。
- 针对 Linux 系统较为安全的方法是只使用密钥登录，禁止密码登录。
- 尚航云_V1平台提供 安全组功能 ，建议您只放行业务协议和端口，不建议放行所有协议所有端口。
- 不建议向公网开放核心应用服务端口访问，例如 mysql、redis 等，您可修改为本地访问或禁止外网访问。
- 如果您的本地外网 IP 固定，建议使用安全组或者系统防火墙设置，禁止除了本地外网 IP 之外的所有 IP 的登录请求。

> **注意：**
>
> 做好日常云服务器系统的安全防护，可以有效加强云服务器系统安全， 但无法保证绝对安全。 建议定期做好云服务器系统的安全巡检及数据备份，以防突发情况导致数据丢失或业务不可用。

如何做好云服务器防范措施？

建议 升级主机安全专业版 并处理中危及以上的安全事件。

木马类问题

主机安全发现漏洞木马等攻击是否会进行通知？

会，若主机安全发现木马、应急漏洞或者其他攻击的行为，会通过站内信、短信、邮件或企业微信的方式进行告警通知，具体方式您可以在 消息中心 进行设置。

未能成功检测出木马（漏报）如何解决？

若发现有未检测出来的木马文件，可通过 工单 联系提交给尚航云_V1安全团队，由尚航云_V1安全团队快速鉴定。

如何处理木马及病毒文件？

- 若发现病毒及木马文件需及时进行隔离或删除相应恶意文件。
- 部分顽固木马、病毒可能存在重复写入的情况，需排查机器上是否存在弱口令、漏洞等异常情况并进行修复，同时删除恶意文件。
- 部分感染型病毒木马极难进行清理，建议定期对机器做快照备份。
- 更多操作，请参见 木马文件操作处理。

异常登录类问题

云服务器显示登录异常怎么解决？

基于管理员的常用登录地进行异常登录判断，请仔细检查登录记录。若非管理员本人登录，密码可能已经泄露，用户需要对云服务器进行详细的安全检查。

如何处理异常登录告警？

1. 首先确认该异常登录是否为业务相关人员进行的登录，若非业务相关人员登录，在控制台确认是否存在木马、漏洞及源占用异常等情况，若有异常情况，请及时处理。

2. 确认该登录账户是否存在密码强度较弱的情况，及时进行修改。

3. 排查机器中的登录账号是否存在异常账号或权限过高的账户，及时禁用账户或调整权限。

正常登录行为被误报为异常登录，要如何消除误报？

您可以登录 主机安全控制台，在左侧导航中选择**入侵检测** > **异常登录**，在异常登录页面，找到被定义为异常登录的记录，在右侧操作栏中，单击**加白名单**，通过自定义添加登录白名单，即可消除误报。

是否可以关闭异常登录检测？

不可以关闭异常登录检测。如果您不想接收异常登录的告警通知，您可以将登录来源添加到白名单，或者取消勾选告警通知，操作步骤如下：

- **方式1**：在异常登录页面，选择**白名单管理** > **添加白名单**，将登录来源添加为白名单。

- **方式2**：在**设置中心** > 告警设置页面，取消勾选异常登录的告警项"高危异常"或"可疑异常"即可。

> **注意：**
>
> 如取消勾选，您将不能实时接收到异地登录的告警通知，请谨慎操作。

密码泄露类问题

云服务器被暴力破解如何处理？

若云服务器被暴力破解成功，需尽快排查机器上的异常并进行处理：

- 排查机器中的账户是否存在弱口令，修改口令强度较弱的密码或采用密钥的方式进行登录，同时可通过设置安全组等方式降低被暴力破解的风险。
- 主机安全已上线暴力破解阻断功能，可进行有效拦截。

提示密码被暴力破解成功之后该如何解决?

密码破解成功后，云服务器可能已被黑客入侵并留下了后门程序。

- 检查云服务器安全状况，是否还有其它未知账户和木马文件，如果存在请立即删除和修复，并修改云服务器登录密码。
- 根据实际情况决定是否需要对云服务器进行重置，并设置复杂密码，尽量字母、数字、特殊字符3种组合，长度在15位及以上。

防护状态离线类问题

云服务器的防护状态显示离线要如何解决?

尚航云_V1服务器主机安全客户端未连接服务端，导致后台显示离线，建议重新下载主机安全客户端进行安装，离线的可能原因如下：

- 云服务器启用了防火墙规则。
- 云服务器安装了第三方恶意软件，导致安全防护程序被破坏。

> **说明：**
>
> 故障排查方式请参见 Linux 客户端离线排查 或 Windows 客户端离线排查。

租户端操作指南
安全概览

最近更新时间: 2024-08-23 15:08:00

本文档将为您介绍安全概览各模块功能及操作步骤。

概述

主机安全的安全概览实时展示您的主机安全评分、待处理风险、安全防护状态、风险趋势以及主机安全的实时动态；推送安全播报，方便您了解主机安全最新威胁情报；提供帮助文档和主机安全升级服务建议，帮助您抵御黑客入侵风险及攻击威胁，保障企业主机安全。

操作指南

登录主机安全控制台，在左侧导航中，单击**安全概览**，进入安全概览页面。安全概览界面提供安全概览信息和相关处理操作，各模块功能说明如下：

安全状态

1. 在安全状态功能中，展示您的主机安全评分和安全风险情况，并提供快捷处理入口。且将安全风险划分为4大类：

   - 入侵检测：包括入侵检测模块的7个功能，即文件查杀、异常登录、密码破解、恶意请求、反弹 Shell、本地提权、高危命令，合并统计待处理风险数和受影响主机数。
   - 漏洞风险：包括 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞，合并统计待处理风险数和受影响主机数。
   - 基线风险：只统计基线待处理风险数和受影响主机数。
   - 网络风险：统计攻击事件待处理风险数和受影响主机数。

2. 单击**立即处理**，将打开风险处理详情弹框，可以查看入侵检测、漏洞风险、基线风险和网络风险具体详情。单击对应**风险卡片**，页面将跳转至相对应的风险处理界面。

主机安全状态划分为3个等级：

等级	体检评分	字体颜色	状态说明
优	90分 - 100分	绿色	资产安全状态较好，需继续保持，定期巡检。
中危	60分 - 89分	橙色	资产存在较多安全风险，建议您及时处理安全事件。
高危	20分 - 59分	红色	资产存在严重安全风险，请您尽快处理安全事件。

> **说明：**
>
> 主机安全状态体检评分最低分数为 20分。

按安全事件分类计算扣分项，安全事件等级分类及扣分规则：

安全事件（按事件数计算）	扣分/个	叠加最大扣分
严重	木马、病毒、爆破成功。	50分
高危	高危漏洞、高危基线、异地登录、本地提权、反弹 Shell、高危命令。	10分
中危	中危漏洞、中危基线。	3分
低危	低危漏洞、低危基线。	2分
其他	基础版（非防护状态）。	1分

安全播报

在安全播报功能中，展示相关产品功能更新、行业荣誉、紧急通知和版本发布信息。单击**更多**，显示安全播报每条播报信息。单击**单个播报**内容显示播报详情。

安全防护

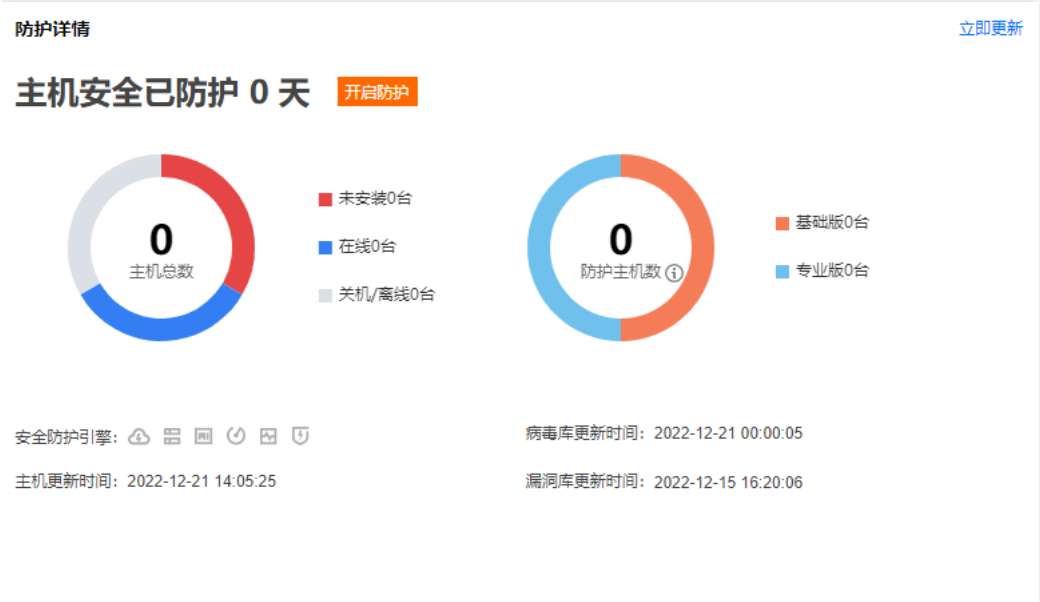
1. 在安全防护功能中，展示主机安全应对入侵攻击提供的（预防-防御-检测-响应）全流程解决方案，并细化展示各阶段所需的安全防护项。若各防护项均开启，可直观了解您当前主机安全的情况，并提供安全风险快捷处理入口。

2. 单击右上角**云原生安全预警**，安全预警页面以大屏的形式展示资产防护状态、安全状态、主机安全防护、安全播报、紧急通知、全网热点威胁，更直观展示主机安全状态助您保卫主机安全。

防护详情

在防护详情功能中，可查看目前主机总数、在线主机总数量、关机或离线的主机数量、未安装客户端的主机数，目前已防护主机数、专业版数量、基础版数量、日志分析使用情况和网页防篡改授权数量，同时提供资产更新时间、病毒库更新时间、漏洞库更新时间以及安全引擎防护等信息。

> 说明：
>
> 由于基础版主机防护程度相对较弱，“已防护主机数”仅包含专业版主机。



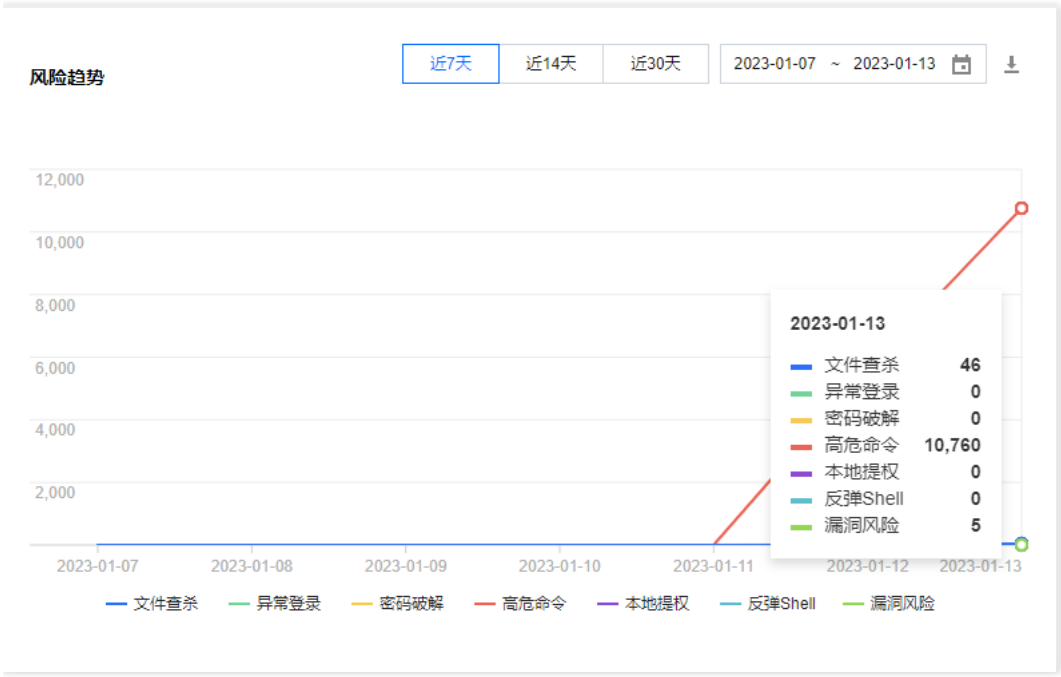
字段说明：

- 单击右上方**立即更新**，可更新资产信息。
- 单击右上方**版本对比**，展示主机安全产品提供的基础版、专业版、增值服务防护的功能对比。
- 在未安装客户端主机中，单击**安装**，界面展示安装引导。
- 单击日志分析右侧的**升级扩容**或网页防篡改右侧的**购买授权**，可购买对应的服务。
- 在基础版主机中，单击**升级**，将跳转到主机安全购买页面，您可以通过购买对基础版主机进行升级，为您的主机提供更为强大的风险威胁抵御能力。
- 安全引擎防护将展示6个引擎图标，分别代表云查杀引擎、BinaryAI 引擎、TAV 引擎、异常行为、威胁情报、攻击防御。若未开启防护功能，对应功能图标处于灰色状态。若有任意一台主机，开通防护功能，则对应功能图标处于点亮状态。

风险趋势

风险趋势功能通过折线图，为您展示近7天、近14天或近30天的安全风险和威胁发生趋势，并且支持按时间段筛选查看。将鼠标在趋势图中悬停，将显示该日期文件查杀、密码破解、异常登录、漏洞风险、基线风险等安全事件数。单击右上角，支持将所选中日期的安全事件数下载至本地。

> 说明：
>
> 数据来源为当日新增待处理事件数，每小时更新一次，历史事件数将保留，不再变更。



实时动态

实时动态功能按照时间倒序实时展示发现的主机风险及威胁事件。单击蓝色字段的**主机 IP**，页面跳转至"主机详情页"的相应子页面；单击事件动态右侧**查看详情**，将跳转至相应事件处理页面。

资产概览

最近更新时间: 2024-08-23 15:08:00

资产管理可视化统一管理主机列表，助您全面了解自身资产运行情况。本文档将为您介绍资产管理功能特性。

前提条件

仅专业版主机支持资产指纹数据采集和同步，基础版或未防护主机须升级专业版才可使用该功能。各版本功能特性详见功能介绍与版本比较。

背景信息

- 资产管理概览、主机列表、组件列表的数据每隔8小时自动同步一次，支持手动同步。
- 资产指纹支持采集以下十种指纹的信息：资源监控、账号、端口、进程、软件应用、数据库、Web应用、Web服务、Web框架、Web站点。

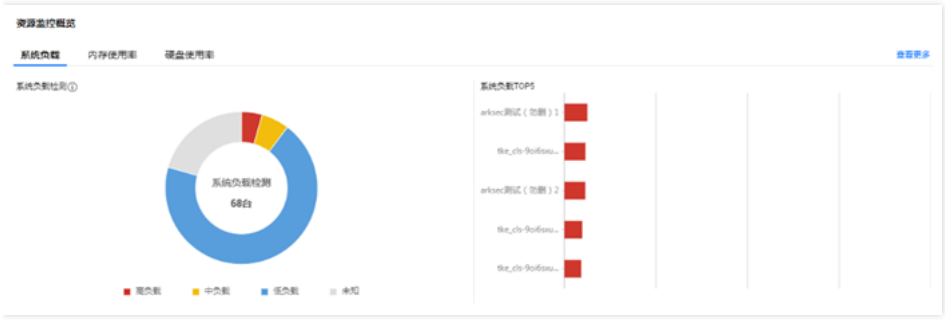
概览

登录主机安全控制台，在左侧导航栏，选择**资产管理**>**概览**，进入概览页面。

1. 资产概况面板，可查看全部主机及各项资产指纹的统计情况。

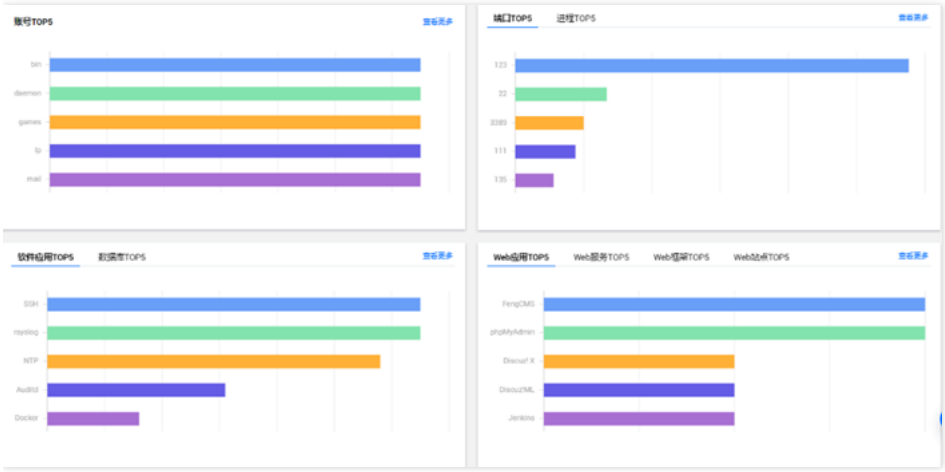
2. 主机概况趋势图（总台数、在线台数、离线台数、风险台数）支持最长不超过近3个月时间段的查询，支持下载导出；主机标签 TOP 5，可查看所有主机中使用最多的前5个标签。

3. 资源监控概览，可查看系统负载、内存使用率、硬盘使用率的分布情况及相应TOP 5。



> **说明：**
>
> 系统负载，仅支持获取 Linux 系统的服务器系统负载，Windows 系统的暂认定为未知。

4. 查看账号TOP 5、端口TOP5、进程TOP 5、软件应用TOP 5、数据库TOP5、Web应用TOP 5、Web服务TOP5、Web框架TOP 5、Web站点TOP5。

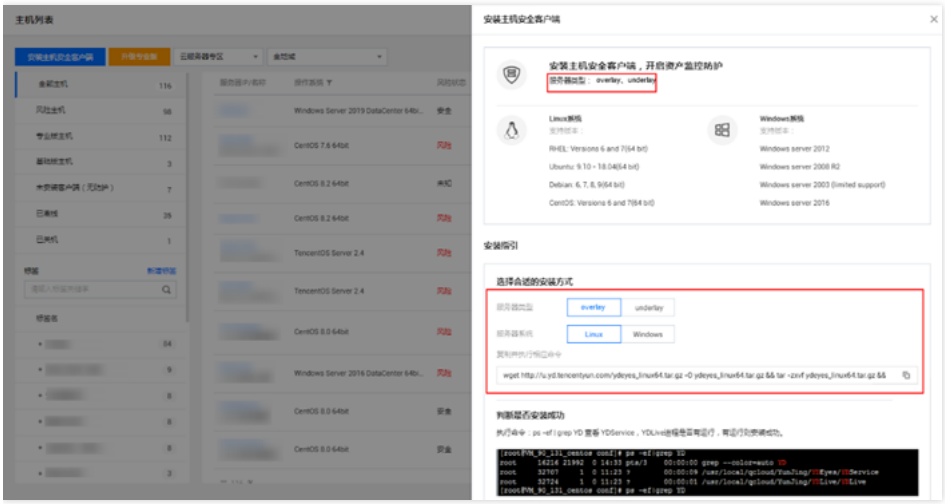


> **说明：**
>
> 各资产指纹TOP 5是根据指纹（账号、端口、进程、软件应用、数据库、Web应用、Web服务、Web框架、Web站点）所属服务器数量降序排列后，取排名前5项的数据。

主机列表

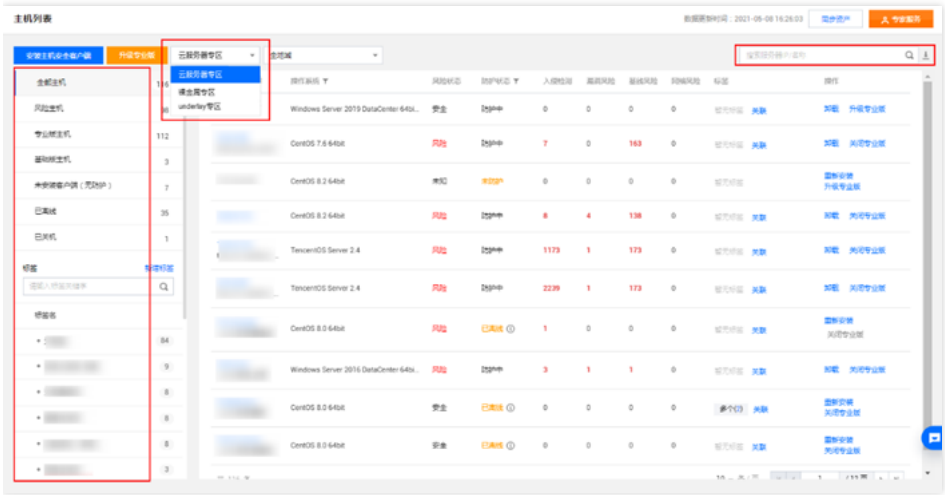
登录主机安全控制台，在左侧导航栏，选择**资产管理**>**主机列表**，进入主机列表页面。

- 安装主机安全客户端
  - 支持混合云机器即 overlay 服务器（云服务器、裸金属）、underlay 服务器接入主机安全。
  - 可根据所要安装客户端的机器属性，选择合适的安装方式安装主机安全，安装完成后，须验证是否安装成功。

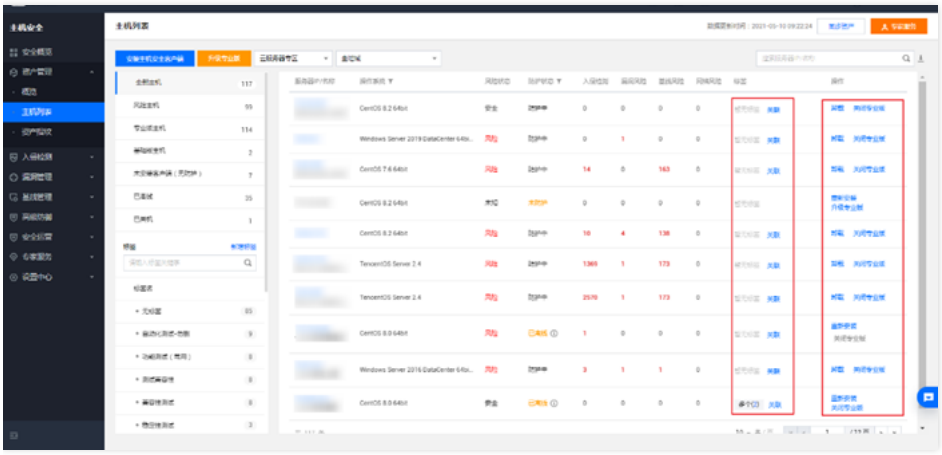


机器不论是 overlay 或 underlay，均只有专业版机器会提供相关安全功能，详见功能介绍与版本比较。

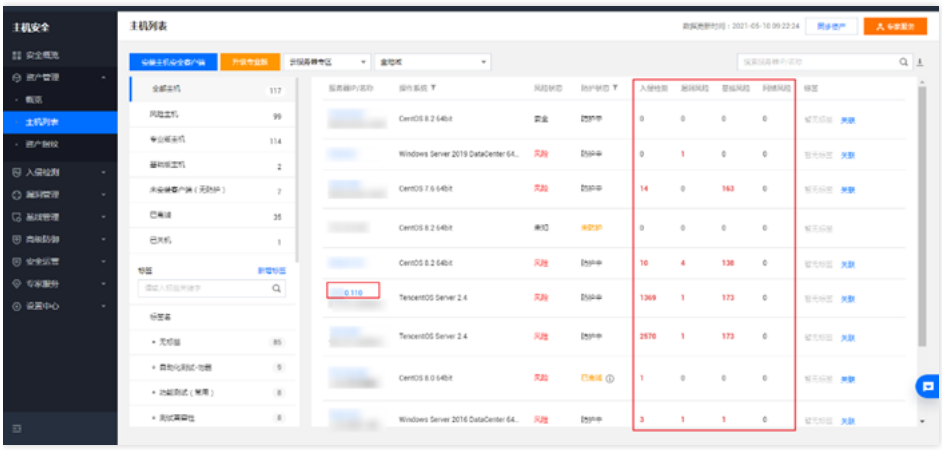
- 升级专业版 点击“升级专业版”按钮跳转专业版购买页
- 筛选导出
  - 支持联动筛选服务器专区（云服务器专区、裸金属专区、underlay专区）、地域、主机状态（全部主机、风险主机、专业版主机、基础版主机、未安装客户端、已离线、已关机）、标签及服务器IP或名称搜索。
  - 点击导出按钮，可对当前筛选出来的机器进行数据导出。

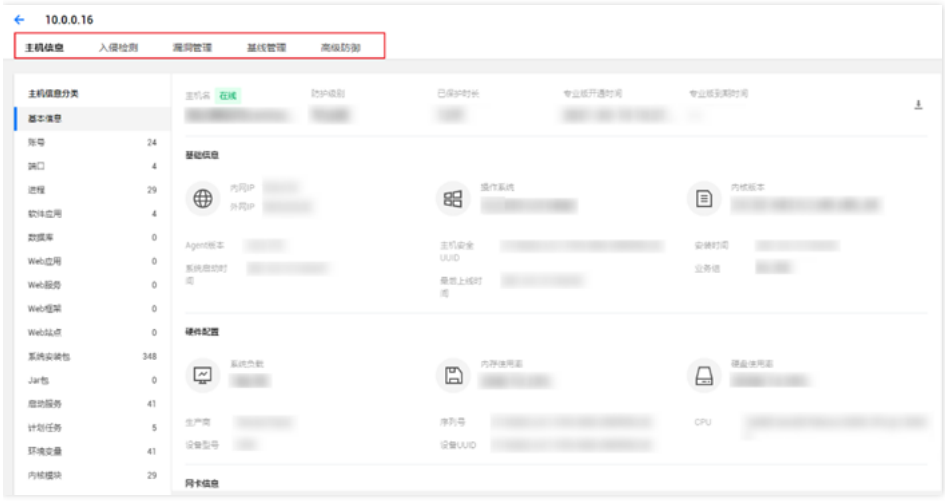


- 主机列表
  - 支持设置标签、关联标签；支持重装/卸载主机安全客户端、升级/关闭专业版。



- 点击蓝字服务器IP可跳转查看该主机详情，点击入侵检测、漏洞风险、基线风险、网络风险数值可跳转查看详情。



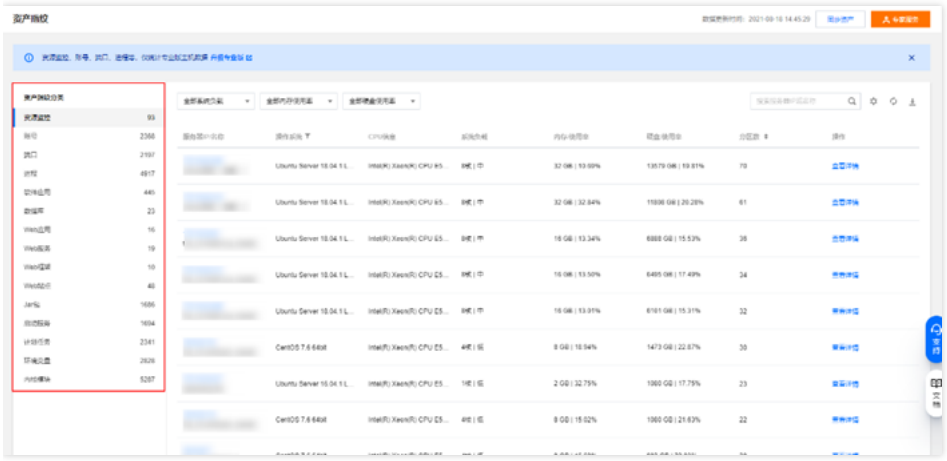


仅专业版的主机详情支持展示资产指纹相关信息。

资产指纹

登录主机安全控制台，在左侧导航栏，选择**资产管理**>资产指纹，进入资产指纹页面。

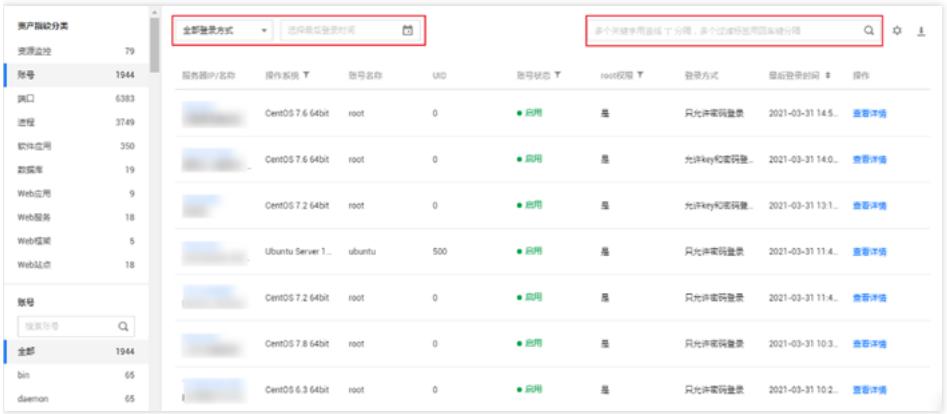
- 资产指纹分类
  - 左侧展示了资产指纹分类列表，包括各资产指纹项及其对应服务器数量。
  - 在左侧资产指纹分类列表中选中一项后，右侧将展示该指纹详情，支持对指纹数据的查询和导出。



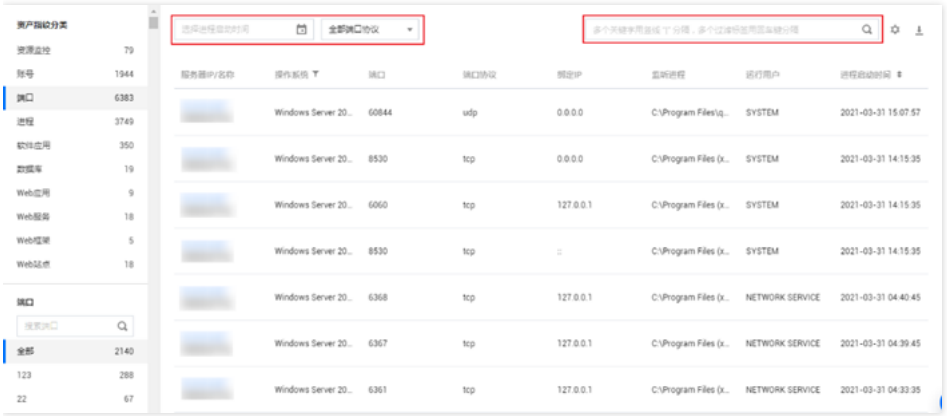
各资产指纹搜索功能均支持模糊搜索。

- 资源监控：对服务器系统负载、内存使用、硬盘使用进行数据采集。

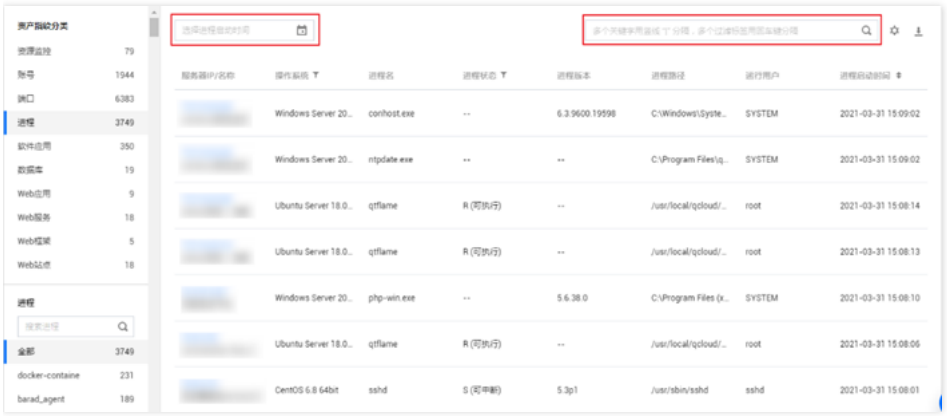
- 账号：对服务器所有账号进行采集。



- 端口：对服务器所有已使用端口进行采集。

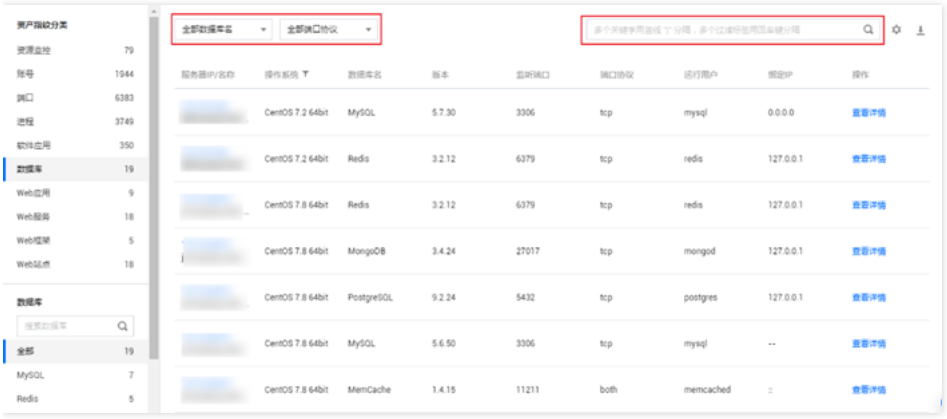


- 进程：对服务器的所有运行进程进行采集。

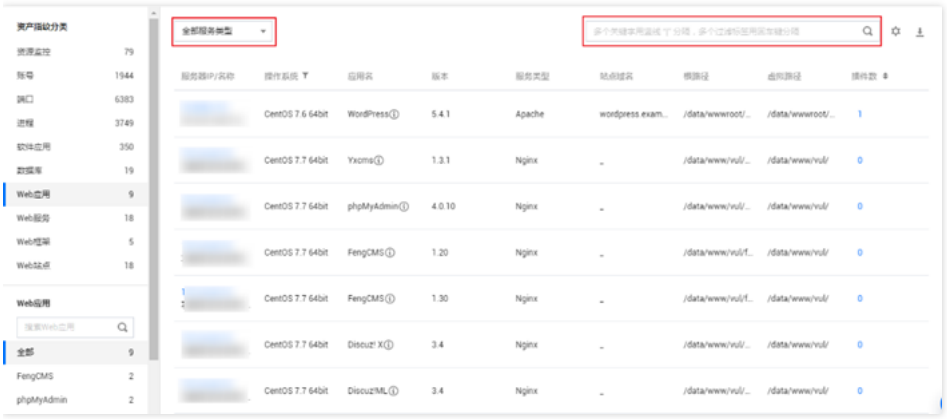


- 软件应用：对服务器所有运行中的软件应用进行采集。

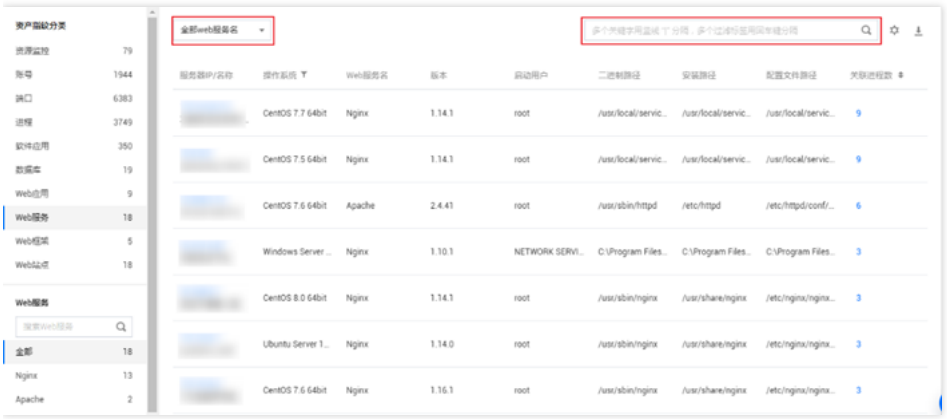
- 数据库：对服务器所有运行的数据库进行采集。



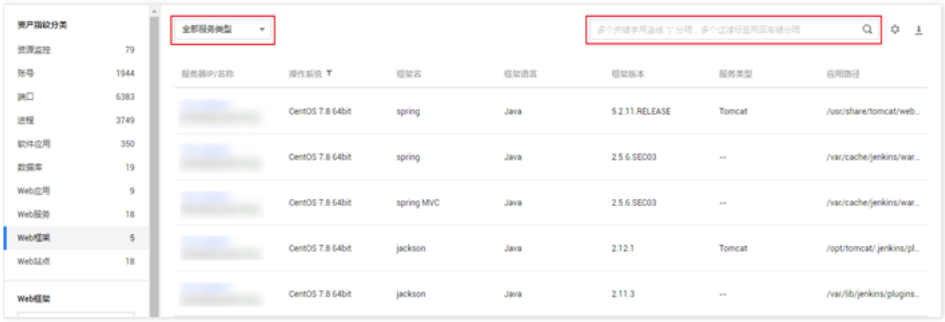
- Web应用：对服务器所有运行的Web应用进行采集。



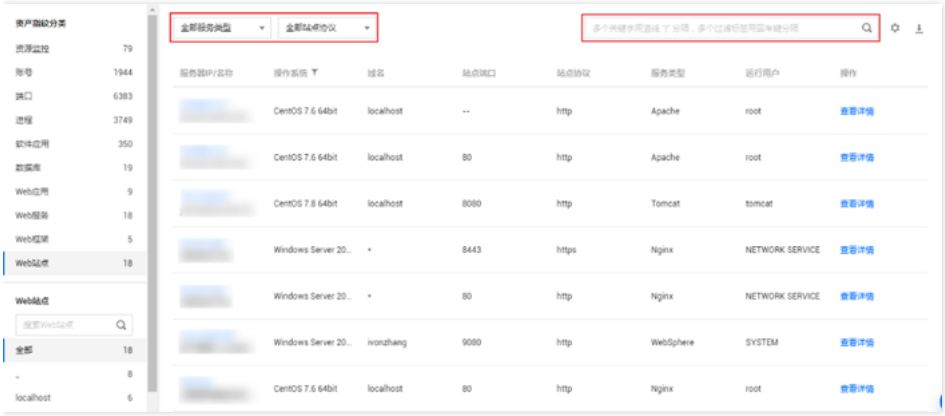
- Web服务：对服务器所有运行的Web服务进行采集。



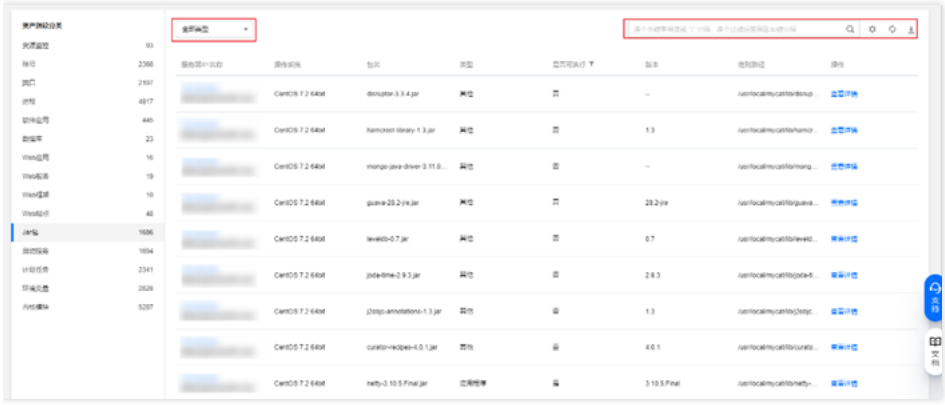
- Web框架：对服务器所有应用的Web框架进行采集。



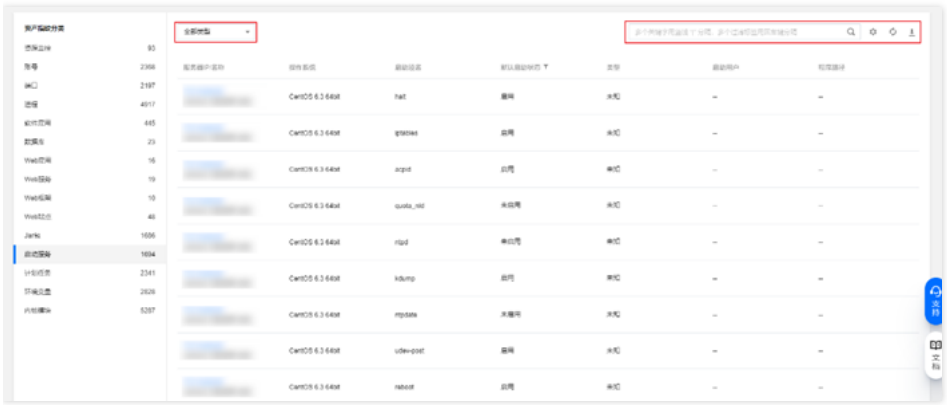
- Web站点：对服务器所有部署的Web站点进行采集。



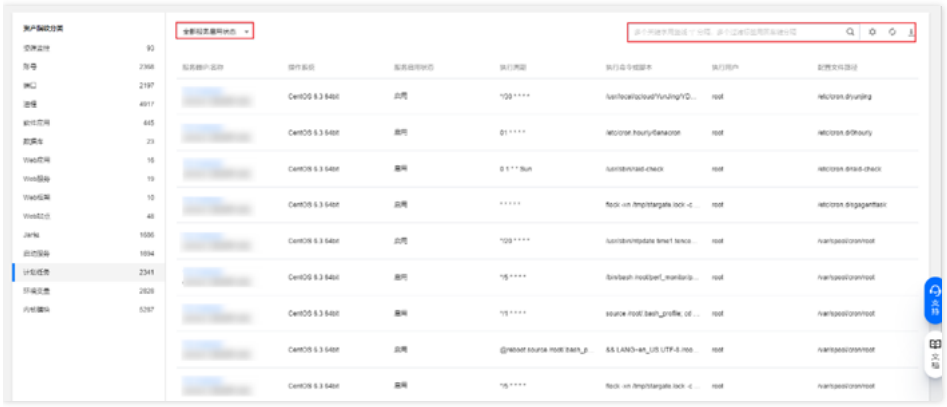
- Jar包：对服务器所有Jar包进行采集。



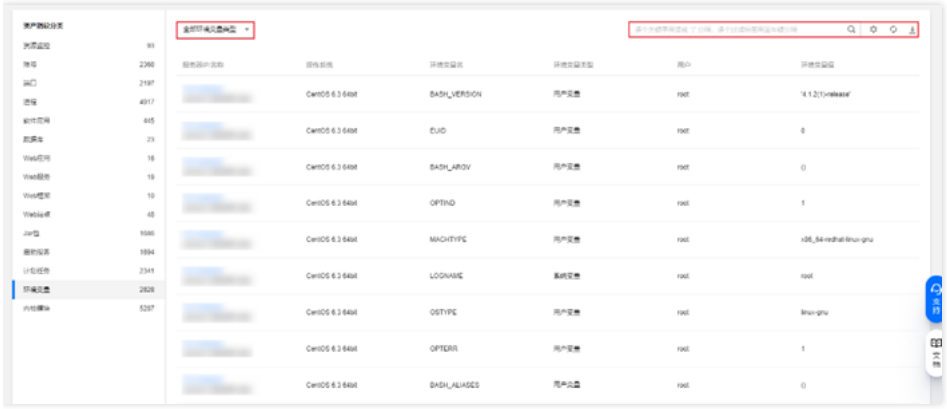
- 启动服务：对服务器所有服务进行采集。



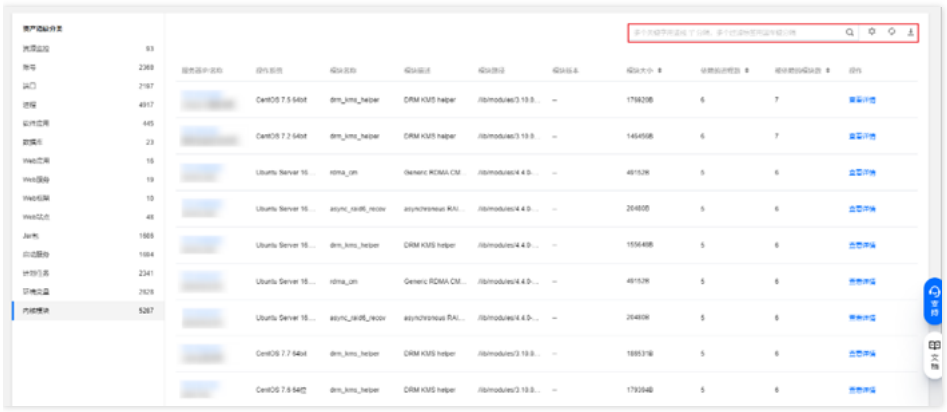
- 计划任务：对服务器所有计划任务进行采集。



- 环境变量：对服务器所有环境变量进行采集。



- 内核模块 ：对服务器所有内核模块进行采集。



主机列表

最近更新时间: 2024-08-23 15:08:00

本文档将为您介绍主机列表各功能模块及操作。

概述

主机列表可查看目前已接入主机安全的所有服务器的信息，帮助您全面了解资产的安全状态。

相关限制

主机安全用户均可查看主机列表，支持混合云服务器接入：

- 云平台：云服务器、轻量应用服务器、黑石物理服务器、边缘计算机。
- 非云平台：其他云服务器、私有云服务器。

操作步骤

1. 登录主机安全控制台，在左侧导航栏，选择**资产中心** > **主机列表**。

2. 在主机列表页面，可以执行查询资产状态、安装主机安全客户端、升级版本等操作。

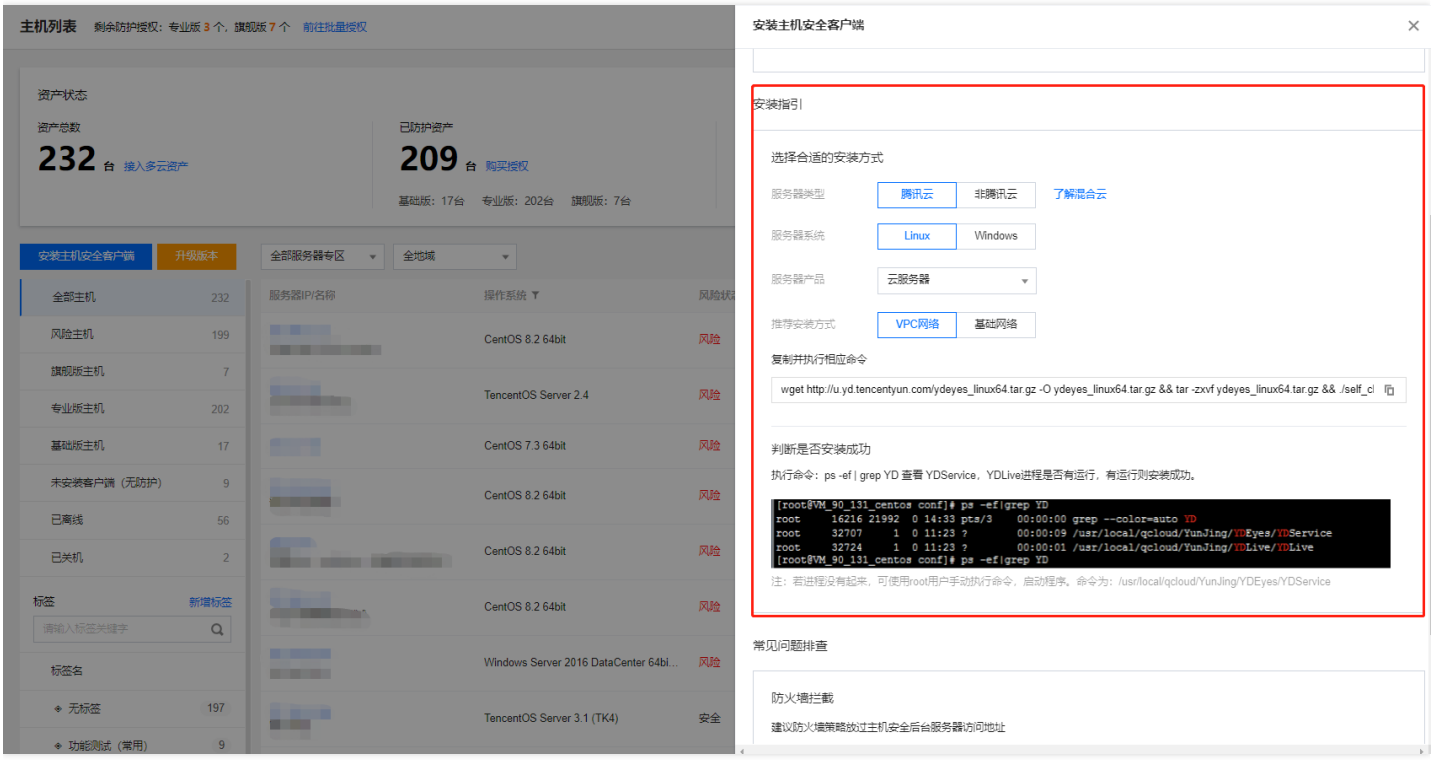
资产状态

在资产状态功能中，可查看目前资产总数、已防护资产（由于基础版主机防护程度相对较弱，此处仅包含专业版主机数）、存在风险的资产数量、未防护资产数量和即将到期的资产数量。

安装主机安全客户端

- 提供主机安全客户端安装指引，可支持混合云机器即云平台（云服务器、黑石服务器、轻量应用服务器、边缘计算机）、非云平台（其他云服务器、私有云服务器）接入主机安全。
- 根据所要安装客户端的服务器属性（服务器类型、服务器系统等）进行正确操作，安装完成后，须验证是否安装成功。

> **说明：**
>
> 服务器不论是云平台或非云平台，均只有专业版服务器可使用相关安全功能。



升级版本

单击**升级版本**将跳转至 购买页，您可根据业务需要对主机安全进行选购。

筛选导出

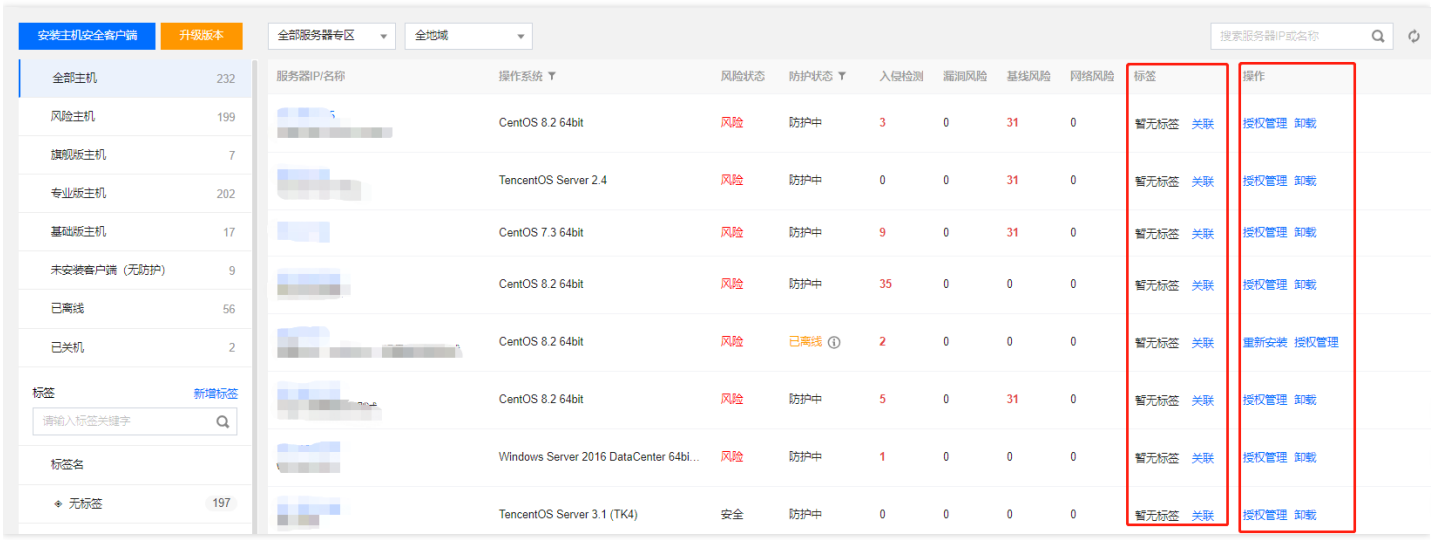
- 支持筛选服务器专区（云服务器、黑石服务器、轻量应用服务器、边缘计算机器、非云平台机器）、地域、主机状态（全部主机、风险主机、专业版主机、基础版主机、未安装客户端、已离线、已关机）、标签及服务器 IP 或名称搜索。

- 单击 导出按钮，可对当前筛选出来的机器进行数据导出。

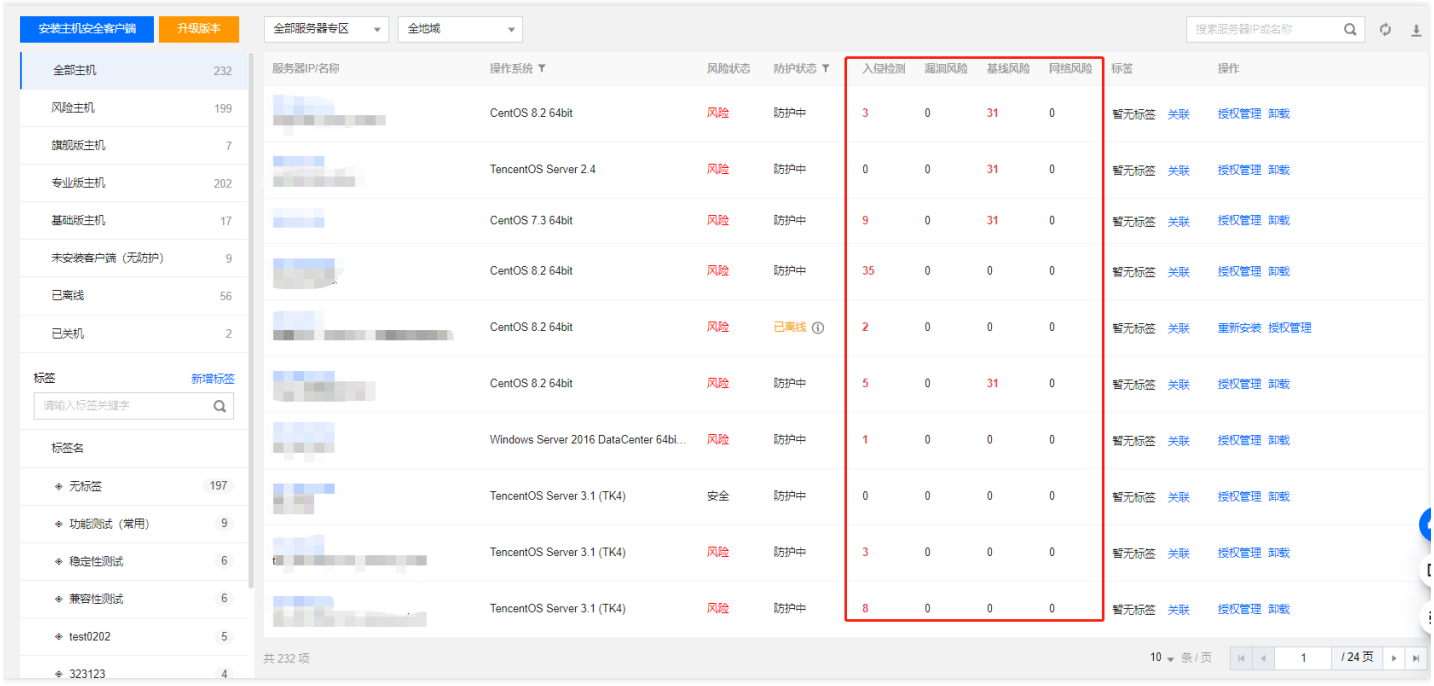
列表操作

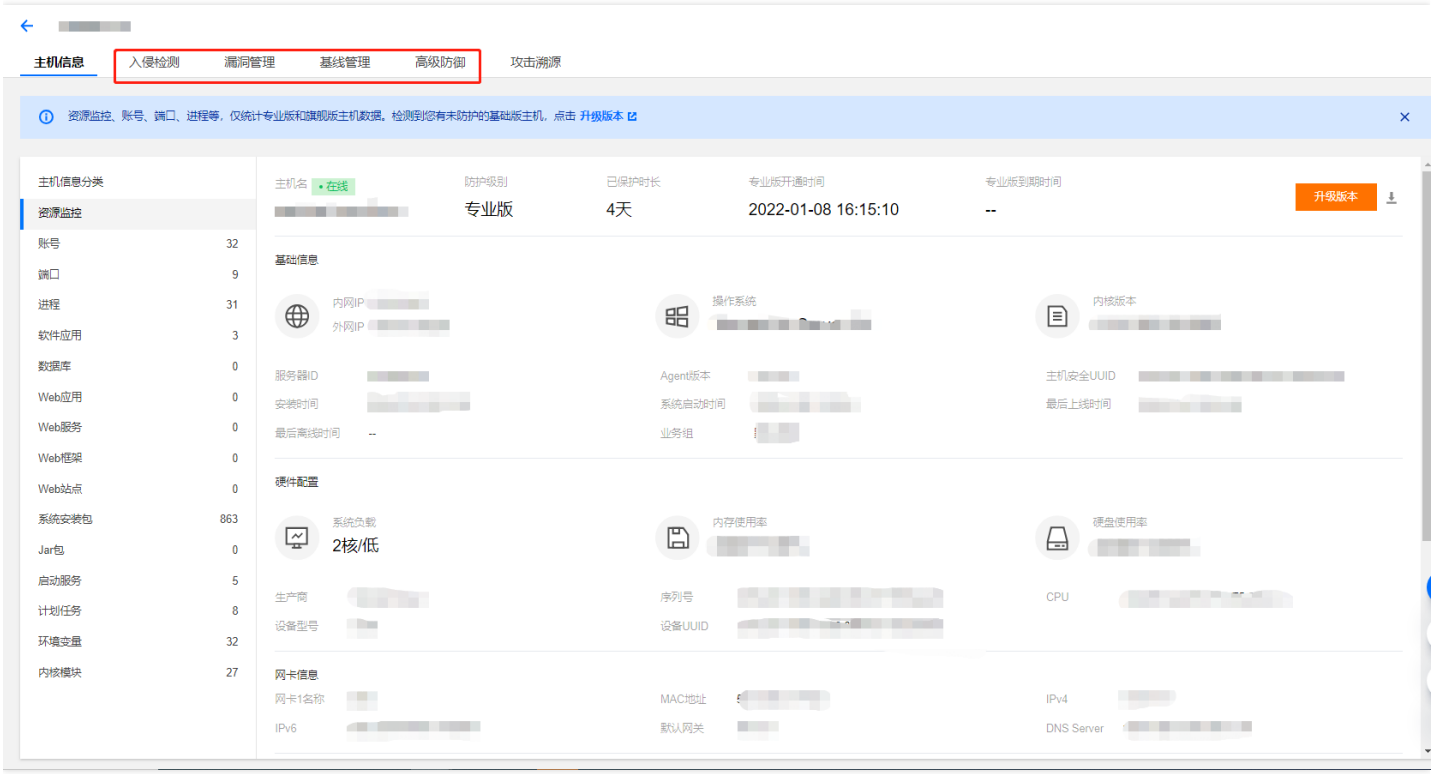
- 支持设置标签、关联标签。

- 支持重装/卸载主机安全客户端、授权管理，单击**授权管理**将跳转至授权管理页，进行版本授权换绑、解绑等操作。

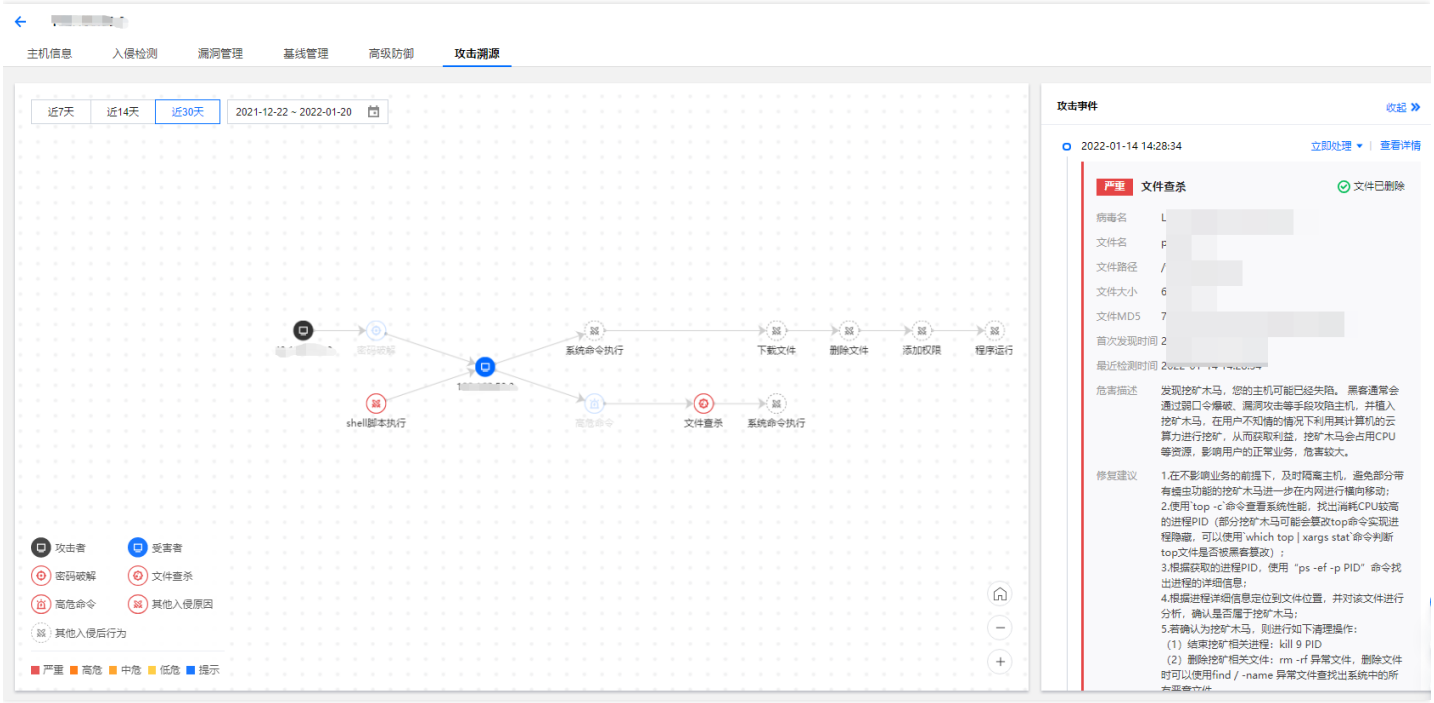


- 单击入侵检测、漏洞风险、基线风险、网络风险的**数值**可跳转查看风险详情。





- 单击**攻击溯源**，支持可视化查看攻击事件。



操作说明：

- 左侧展示针对当前主机的全部攻击情况，以攻击链串联展示，右侧展示针对本台主机的攻击事件详情。
- 在左侧选择单个攻击者链路上的事件时，单条链路点亮，右侧卡片展示单条攻击链来源、描述详情，下方展示单条攻击链内容，并自动定位至具体时间内容，可滚动查看完整攻击链。

- 针对于具体的攻击事件可直接处理和查看详情。

资产指纹

最近更新时间: 2024-08-23 15:08:00

本文档将为您介绍如何查看资产指纹统计数据。

概述

资产指纹数据采集，可帮助您快速了解资产的概况和运行状态。

相关限制

仅付费防护版本的主机才可采集资产指纹数据，基础版主机须先升级版本。

各版本支持采集的资产指纹如下：

主机安全防护版本	采集的资产指纹项
基础版（免费）	不支持
普惠版（仅限轻量应用服务器）	5项：资源监控、账号、端口、进程、软件应用
专业版	10项：资源监控、账号、端口、进程、软件应用、数据库、Web应用、Web服务、Web框架、Web站点

> **说明：**
>
> 资产指纹数据每隔8小时自动采集一次，支持手动采集。

操作步骤

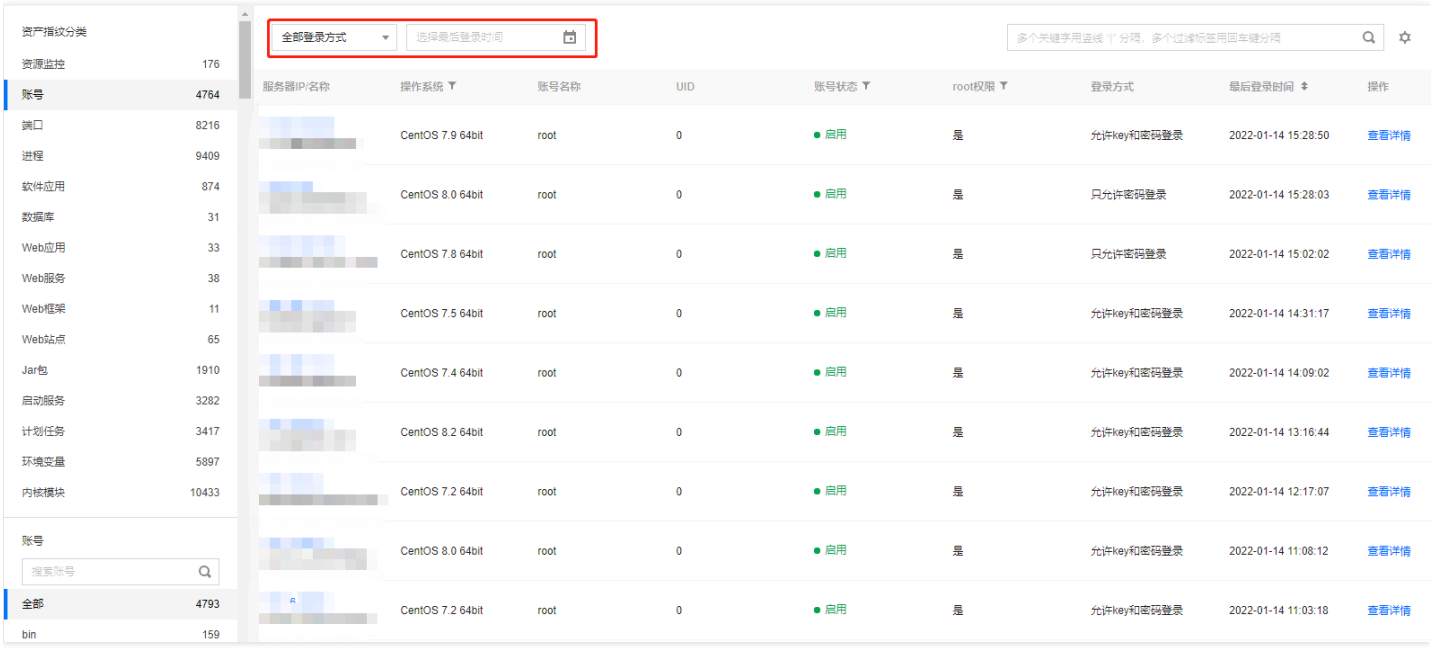
1. 登录主机安全控制台，在左侧导航栏，选择**资产中心** > **资产指纹**。
2. 在资产指纹页面，展示了资产指纹分类列表，包括各资产指纹项及其对应服务器数量。在左侧资产指纹分类列表中选中一项后，右侧将展示该指纹详情，支持对指纹数据的查询和导出。

> **说明：**
>
> 各资产指纹搜索功能均支持模糊搜索。

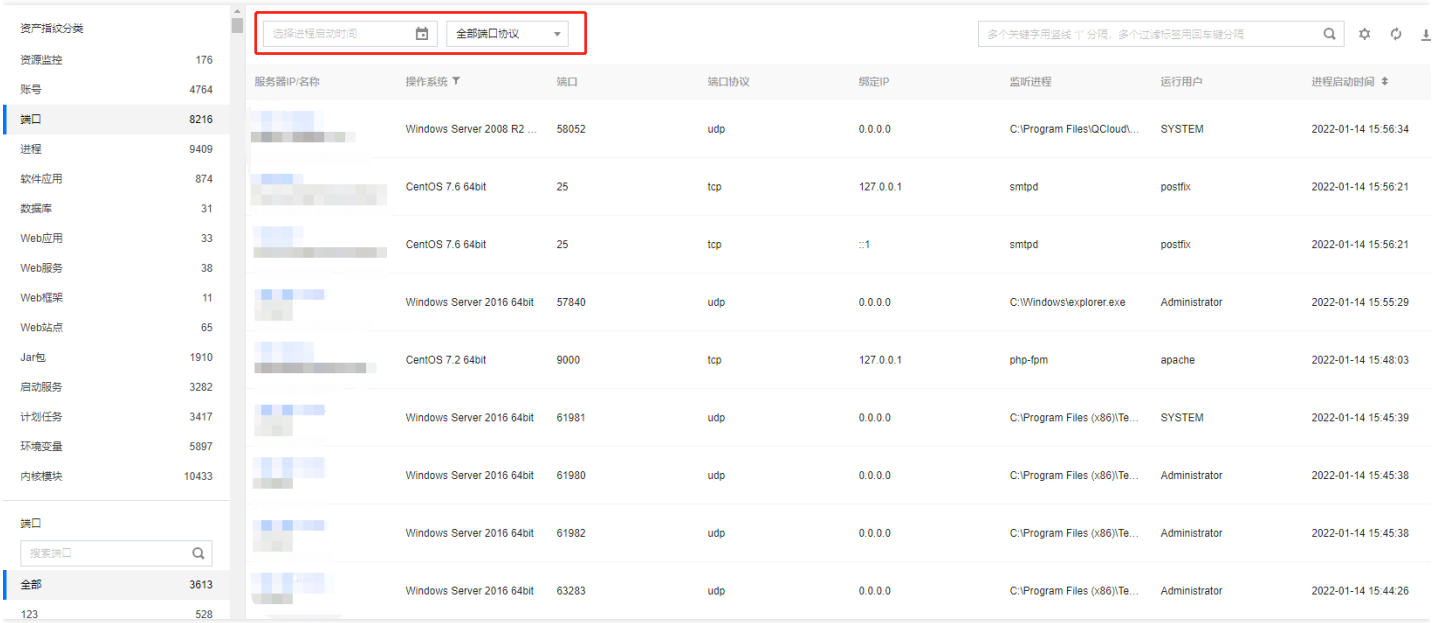
资产指纹分类说明：

- 资源监控：对服务器系统负载、内存使用、硬盘使用进行数据采集。

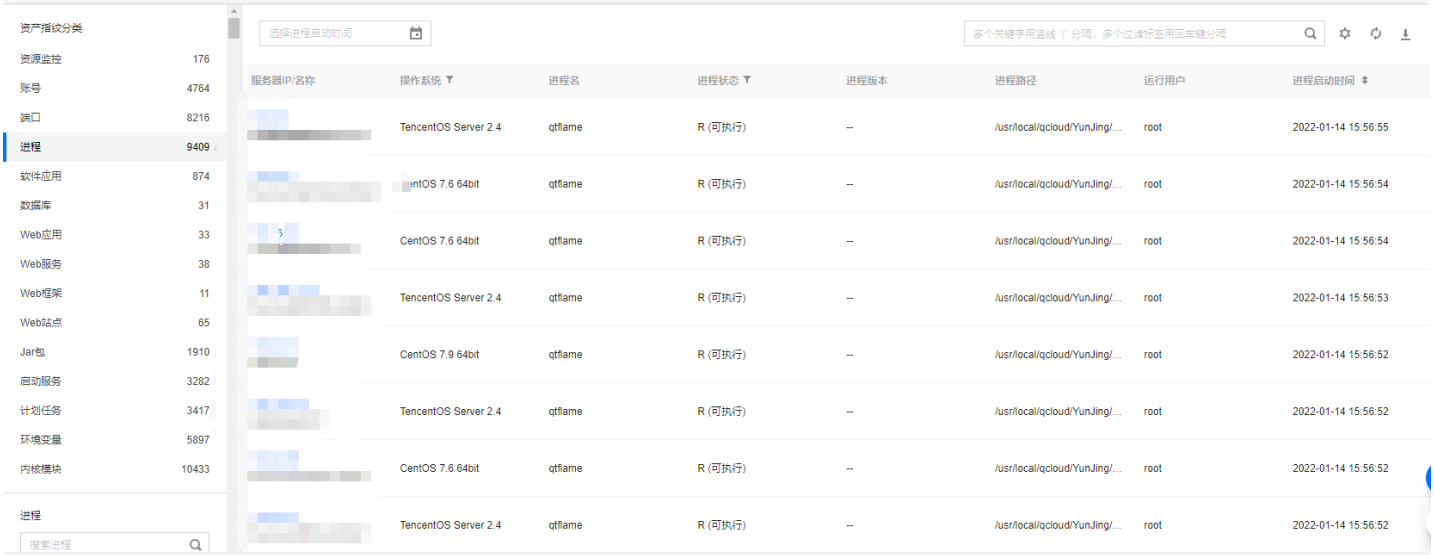
- 账号：对服务器所有账号进行采集。



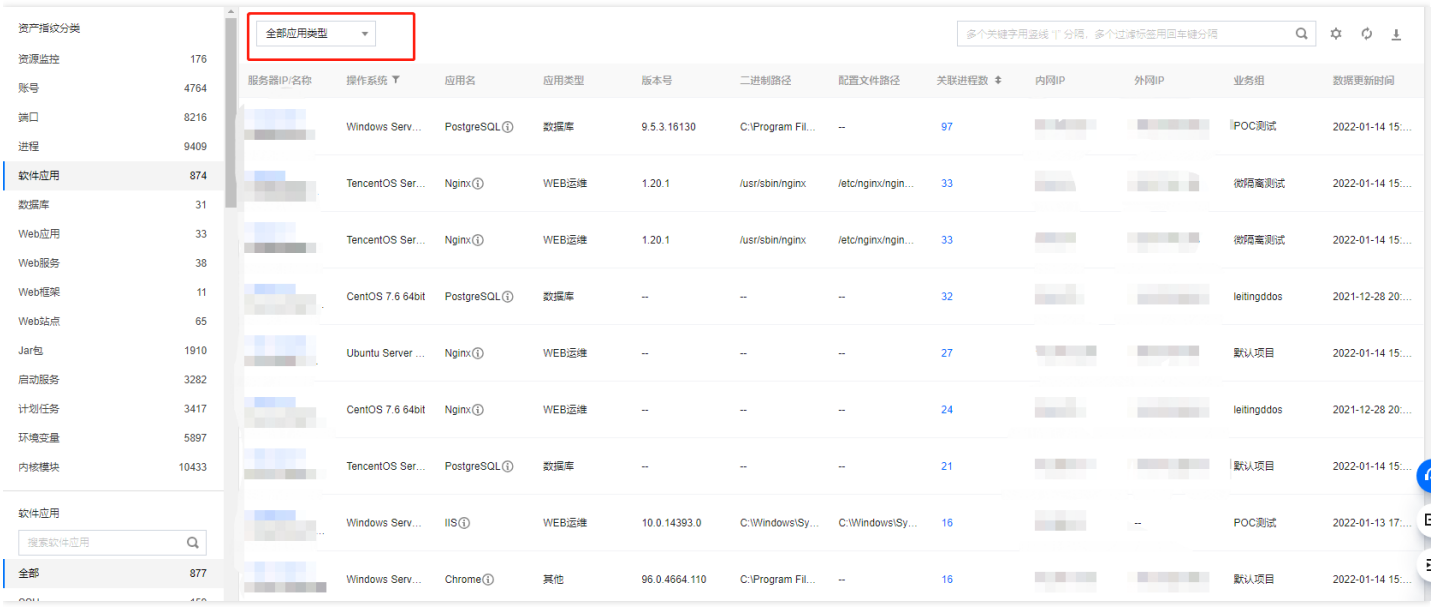
- 端口：对服务器所有已使用端口进行采集。



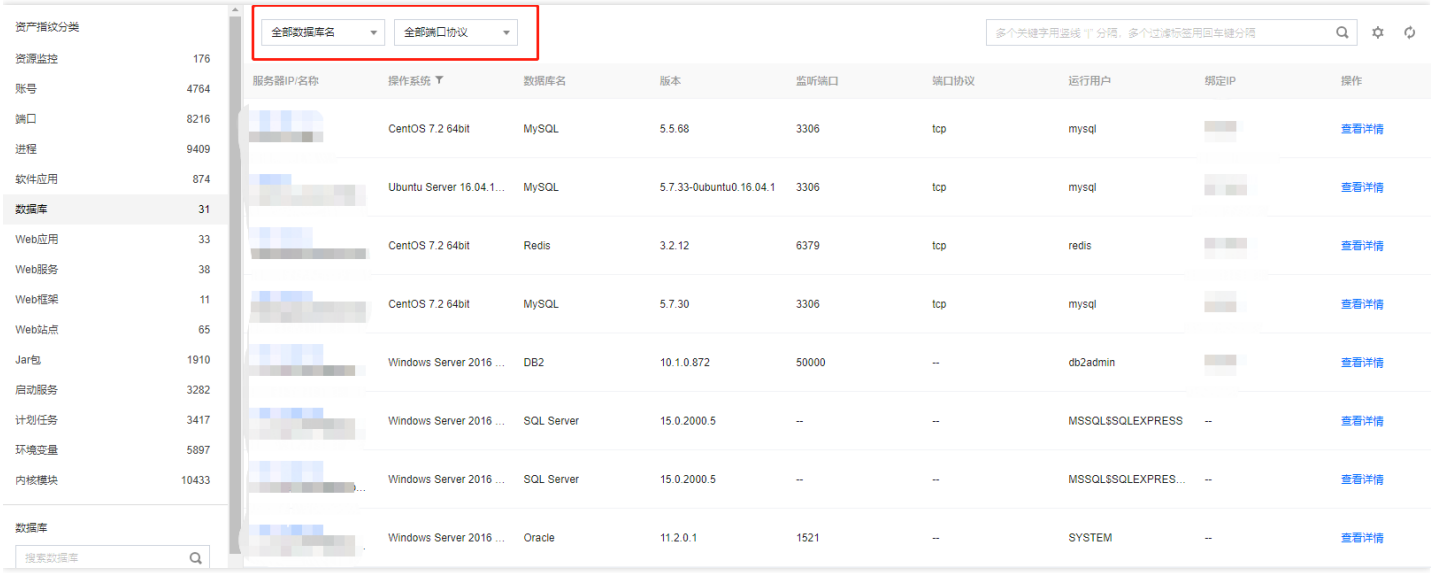
- 进程：对服务器的所有运行进程进行采集。



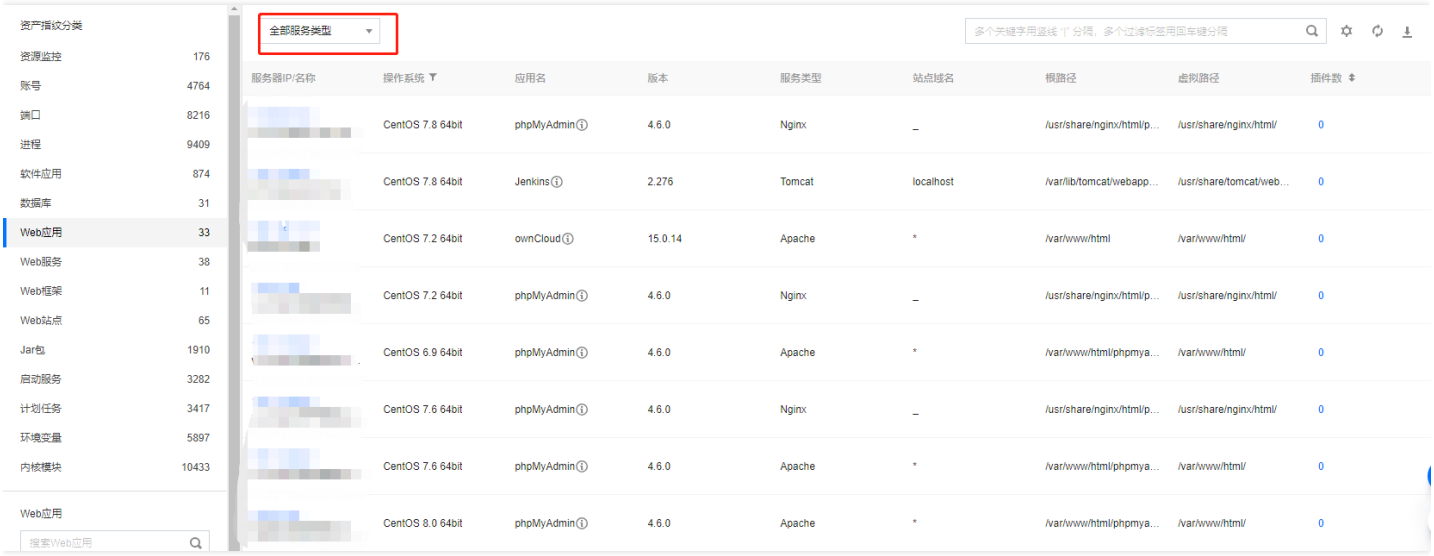
- 软件应用：对服务器所有运行中的软件应用进行采集。



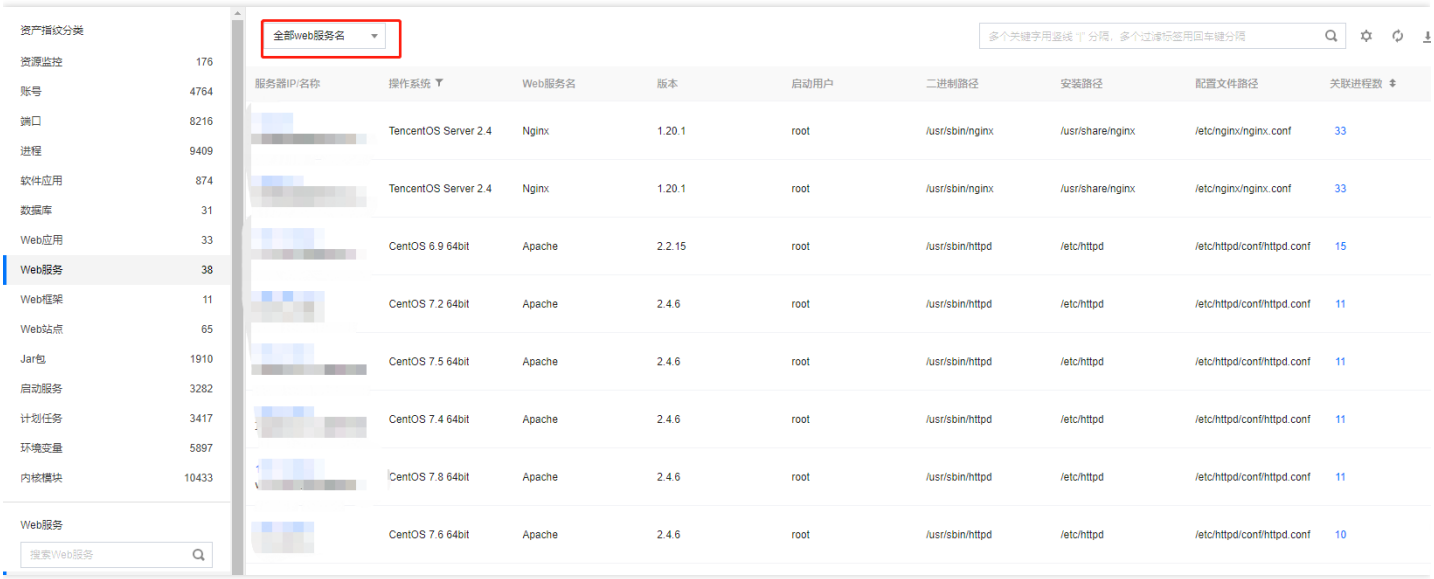
- 数据库：对服务器所有运行的数据库进行采集。



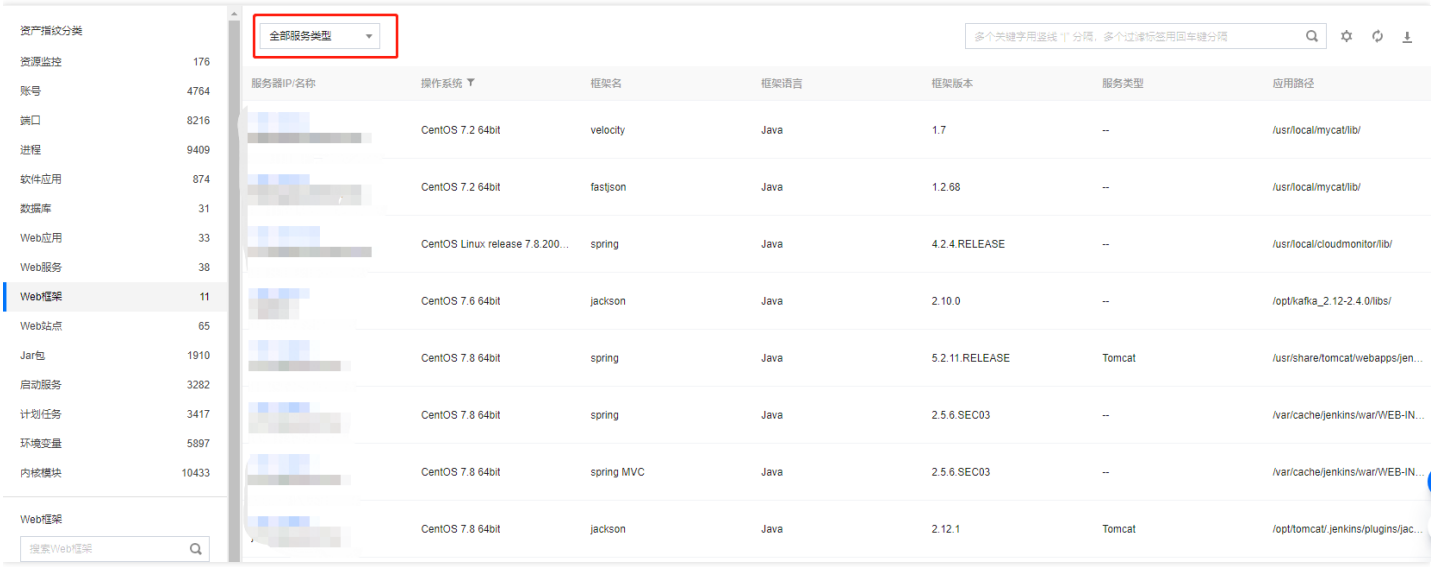
- Web 应用：对服务器所有运行的 Web 应用进行采集。



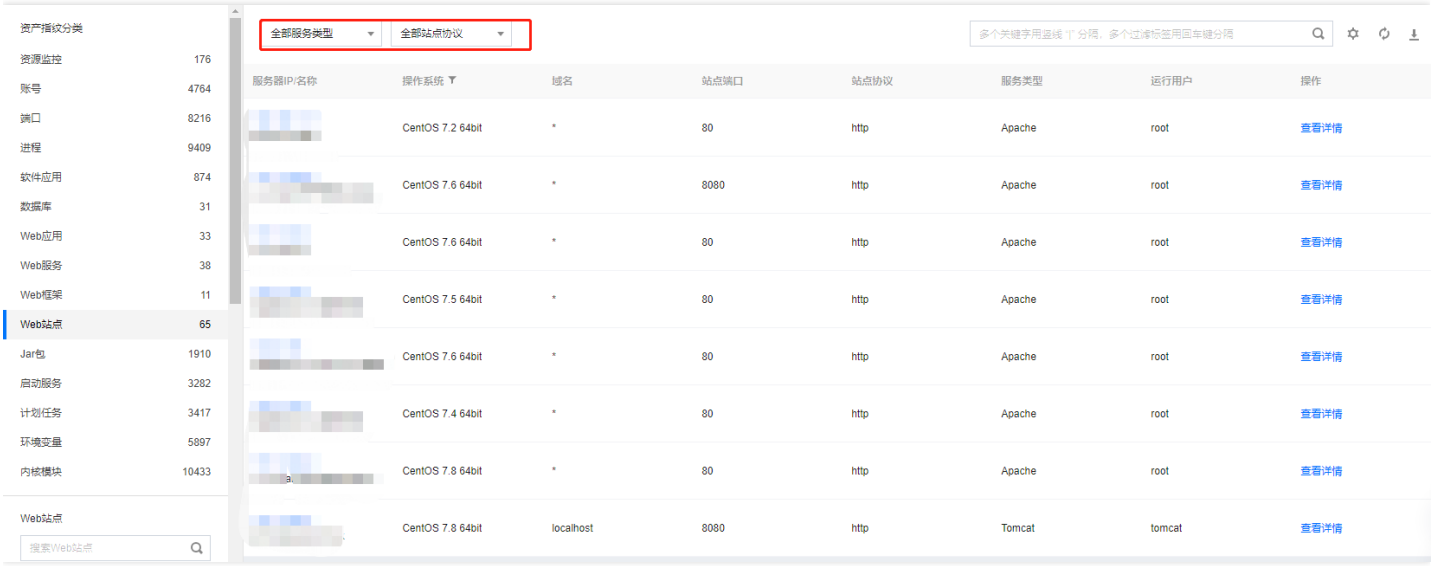
- Web 服务：对服务器所有运行的 Web 服务进行采集。



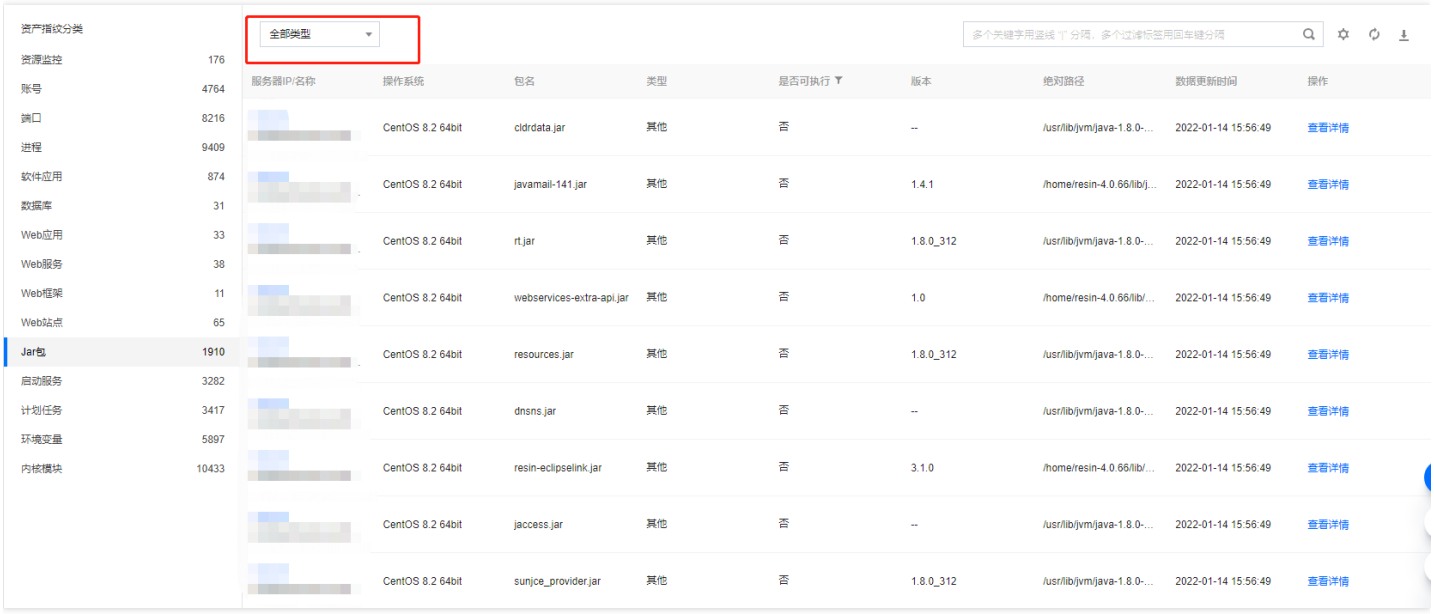
- Web 框架：对服务器所有应用的 Web 框架进行采集。



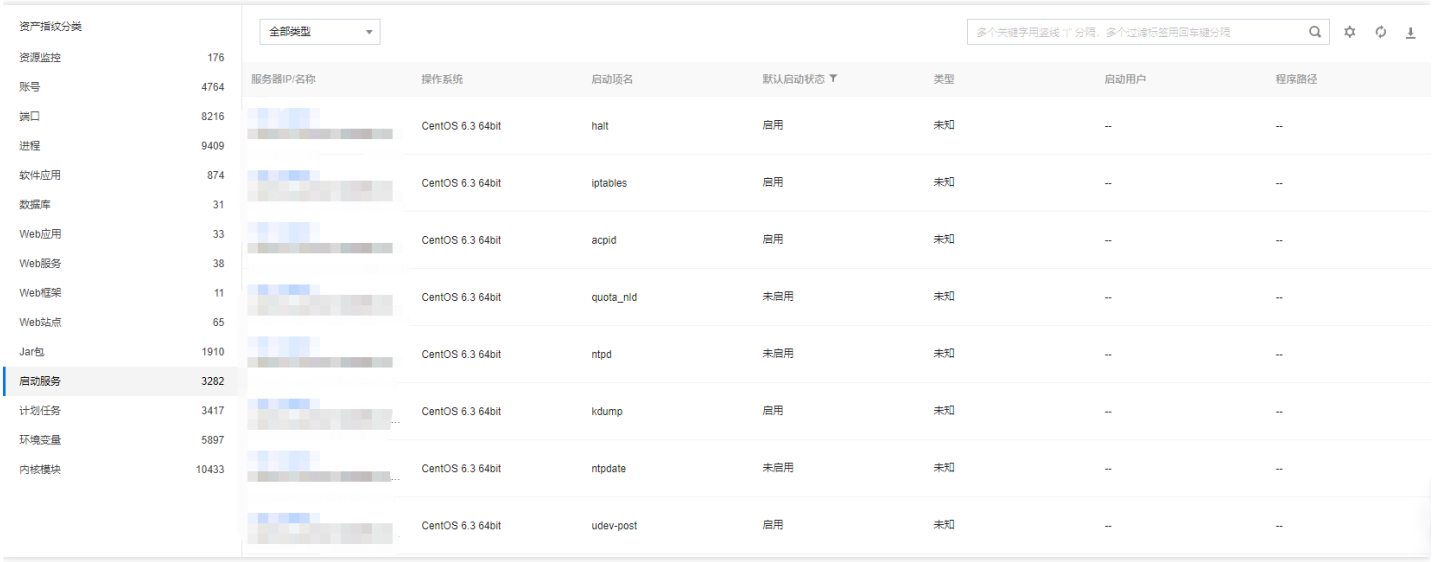
- Web站点：对服务器所有部署的Web站点进行采集。



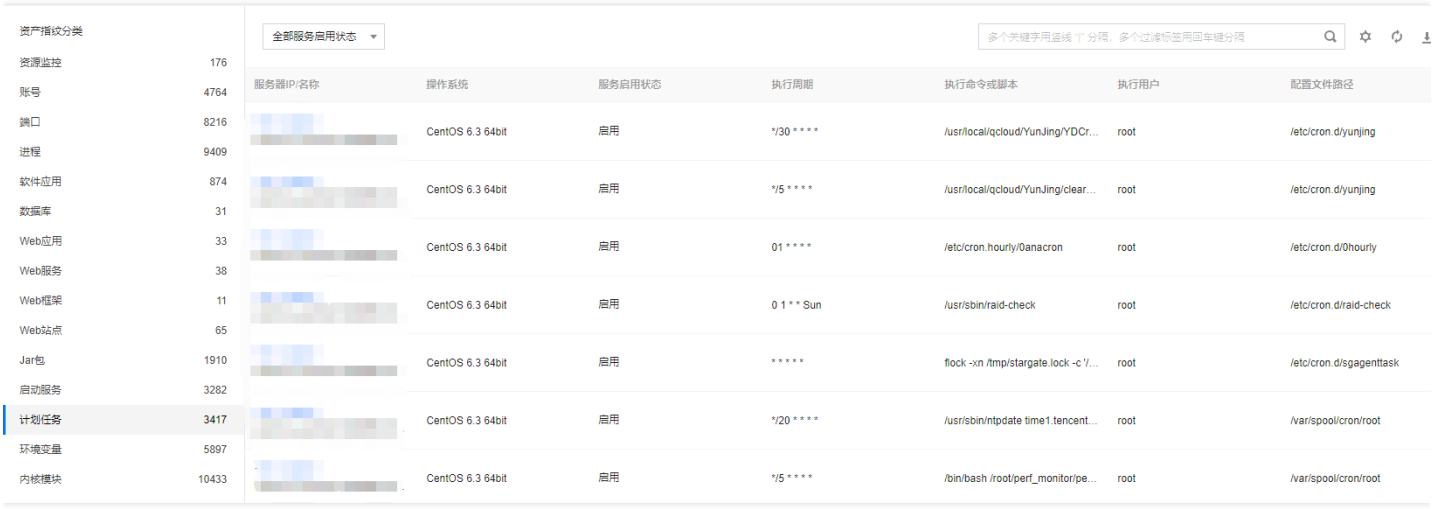
- Jar 包：对服务器所有的 Jar 包进行采集。



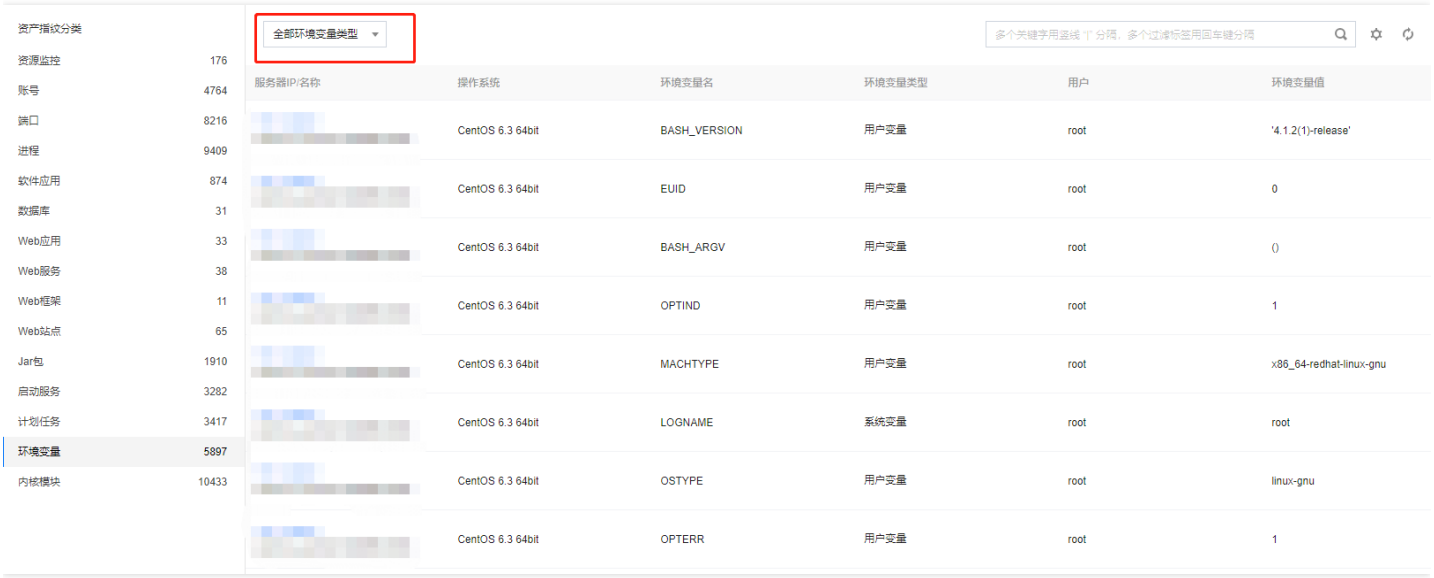
- 启动服务：对服务器所有的启动服务进行采集。



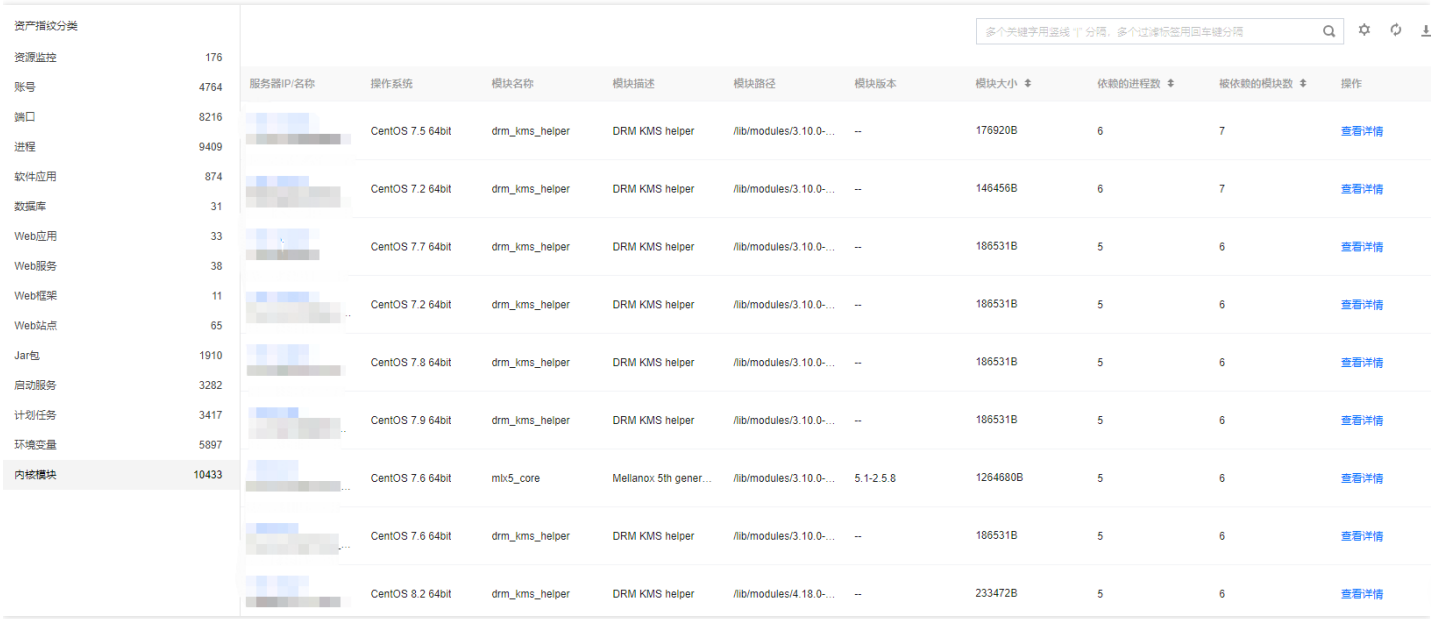
- 计划任务：对服务器所有的计划任务进行采集。



- 环境变量：对服务器所有的环境变量进行采集。



- 内核模块：对服务器的内核模块进行采集。



资产指纹分类

资源监控	176
账号	4764
端口	8216
进程	9409
软件应用	874
数据库	31
Web应用	33
Web服务	38
Web框架	11
Web站点	65
Jar包	1910
启动服务	3282
计划任务	3417
环境变量	5897
内核模块	10433

多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔

服务器IP/名称	操作系统	模块名称	模块描述	模块路径	模块版本	模块大小	依赖的进程数	被依赖的模块数	操作
[redacted]	CentOS 7.5 64bit	drm_kms_helper	DRM KMS helper	/lib/modules/3.10.0-...	--	176920B	6	7	查看详情
[redacted]	CentOS 7.2 64bit	drm_kms_helper	DRM KMS helper	/lib/modules/3.10.0-...	--	146456B	6	7	查看详情
[redacted]	CentOS 7.7 64bit	drm_kms_helper	DRM KMS helper	/lib/modules/3.10.0-...	--	186531B	5	6	查看详情
[redacted]	CentOS 7.2 64bit	drm_kms_helper	DRM KMS helper	/lib/modules/3.10.0-...	--	186531B	5	6	查看详情
[redacted]	CentOS 7.8 64bit	drm_kms_helper	DRM KMS helper	/lib/modules/3.10.0-...	--	186531B	5	6	查看详情
[redacted]	CentOS 7.9 64bit	drm_kms_helper	DRM KMS helper	/lib/modules/3.10.0-...	--	186531B	5	6	查看详情
[redacted]	CentOS 7.6 64bit	mlx5_core	Mellanox 5th gener...	/lib/modules/3.10.0-...	5.1-2.5.8	1264680B	5	6	查看详情
[redacted]	CentOS 7.6 64bit	drm_kms_helper	DRM KMS helper	/lib/modules/3.10.0-...	--	186531B	5	6	查看详情
[redacted]	CentOS 8.2 64bit	drm_kms_helper	DRM KMS helper	/lib/modules/4.18.0-...	--	233472B	5	6	查看详情

文件查杀

最近更新时间: 2024-08-23 15:08:00

本文档将指导您如何在主机安全控制台对木马文件进行操作处理。

文件查杀设置

1. 登录主机安全控制台，在左侧导航栏选择**入侵检测** > **文件查杀**。

2. 在文件查杀页面，单击右上角处的**查杀设置**，右侧弹出查杀设置页面，可对查杀模式进行设置。

> **说明：**
>
> - 该功能属于专业版功能，请先购买防护授权并绑定主机，升级为专业版主机。
> - 文件查杀支持木马文件检测，全部机器可累计免费检测5条恶意文件安全事件，超过则停止检测，升级为专业版主机安全则没有次数限制，常见的木马文件检测有以下两种：
> - Webshell 检测：提供常用的 Web 网站类脚本木马后门检测，包含 ASP/PHP/JSP/Python 等脚本语言。
> - 二进制检测：提供对二进制可执行类的病毒木马检测，例如 DDoS 木马、远控、挖矿类软件等，文件类型包括 exe、dll、bin 等，并告警用户。

3. 在查杀设置页面，支持定时检测、实时监控、自动隔离设置。

- 定时检测：单击开启**定时检测**，设置检测模式、周期和检测范围后，单击**保存**，可定期扫描主机木马病毒文件，增强安全性。

参数说明：

- 检测模式：包括快速检测模式和全盘检测模式，可对运行中进程、关键目录、驱动加载等进行检测。其中全盘检测的时长与服务器磁盘文件数量相关，推荐选择4小时以上，避免出现扫描不完整或超时情况。
- 引擎模式：包括标准模式、增强模式和严格模式。
  - 标准模式：提供精准检测，高效检出主流木马、病毒文件。
  - 增强模式：提供增强检测能力，可检出非主流恶意文件。
  - 严格模式：提供最严格检测能力，命中任何恶意特征将提示用户。
- 检测周期：可选择每天、每隔3天或每隔7天检测周期。
- 检测范围：包括全部专业版服务器和自选服务器。
- 实时监控：单击开启**实时监控**，并选择监控模式后，单击**保存**，可实时监控 Web 目录、系统关键目录，查杀木马病毒文件。

参数说明：

- 监控模式分为标准和推荐两种模式。
  - 标准：监控并扫描检测常见目录下增量文件。
  - 深度：监控并扫描检测所有目录下增量文件。
- 自动隔离：单击开启**自动隔离** > **保存**，自动隔离检测出的恶意文件，部分恶意文件仍需用户手动确认隔离，建议检查文件查杀列表中所有安全事件，确保已全部处理。

> 说明：
>
> 若出现误隔离，请在已隔离列表中对文件进行恢复。开启或关闭自动隔离，均需要进行配置，实际生效存在几分钟延迟。

检测设置概览

1. 登录 主机安全控制台 ，在左侧导航栏选择**入侵检测** > **文件查杀**。

2. 在文件查杀页面，单击**一键检测**，开始设置手动检测模式。

3. 在一键检测设置页面，设置目标检测模式、主机范围和超时时间后，检测可能会因为文件、目录过多、扫描耗时较长，可以设置单次扫描时长，超时则视为扫描失败。

4. 单击开启检测后按照检测设置进行检测，可单击查看详情查看检测详情信息。

检测详情列表包含字段说明如下：

- 影响服务器 ：目标服务器的 IP 及名称。
- 操作系统 ：目标服务器的操作系统。
- 检测状态：目标服务器检测完成、检测中及检测失败的检测状态，其中检测失败的原因可能是目标服务器检测超时失败，建议增加超时时长后重新检测，检测失败的原因可能是客户端已离线，建议重启或重新安装客户端后重新检测。
- 待处理风险：目标服务器检测出待处理的风险文件数量。
- 检测开始时间：此次检测开始的时间。
- 检测结束时间：目标服务器检测结束的时间。
- 操作：
- 重新检测：若想对检测状态处于检测完成、检测停止和检测失败的目标服务器再次检测，您可以单击**重新检测**。
- 停止检测：若想对检测状态处于检测中的目标服务器停止检测，您可以单击**停止检测**。

> 说明：
>
> 选中的服务器将不会被检测，可能存在的风险将不会告警提示，请谨慎操作。

- 查看详情：若想查看目标服务器的检测结果详情，您可以单击**查看详情**。

查看事件列表

1. 登录 主机安全控制台 ，在左侧导航栏选择**入侵检测** > **文件查杀**。

2. 在文件查杀页面，可查看当前受保护的服务器中，木马文件检测情况，如下图所示：

事件列表包含字段说明如下：

- 服务器 IP /名称 ：当前检测的目标服务器 IP 和名称。
- 路径：目标风险文件的文件路径，单击)复制**路径**信息、单击 下载目标风险文件。
- 病毒名/检出引擎：入侵目标风险文件的病毒名。
- 首次发现时间：首次检测到目标风险文件出现的时间。
- 最近检测时间：最近一次检测到目标风险文件出现的时间。
- 处理状态：目标风险文件的处理状态，待处理状态的事件会提示最近一次检测该文件时，文件和进程的存在情况。
- 操作：
  - 隔离：若确认文件是恶意的，可以对单个文件进行隔离，或者批量选择文件进行一键隔离。当隔离成功后，原始恶意文件将被加密隔离，后期可以通过筛选**已隔离**文件，进行恢复。
  - 信任：若文件是非恶意的，可以选择信任操作，加入信任后，主机安全将不再对该文件进行检测，可以通过筛选**信任文件**，对信任文件进行管理。
  - 删除记录：该操作仅删除日志记录，不会删除文件，操作后无法再查看相关日志信息，建议您先对文件进行“隔离”、“信任”操作，或根据路径找到相应文件进行手动删除。
  - 详情：若想查看目标风险文件的检测结果详情，可以单击**查看详情**。

常见问题

木马文件为什么隔离失败？

木马文件隔离失败，一般是由于木马文件对抗安全软件导致的，建议先自行删除服务器中的告警文件。若仍无法处理，请提交工单联系我们进行处理，Windows 系统也可尝试使用腾讯电脑管家进行查杀。

后续步骤

- Linux 入侵类问题排查指南，请参见 Linux 入侵类问题排查思路。
- Windows 入侵类问题排查指南，请参见 Windows 入侵类问题排查思路。

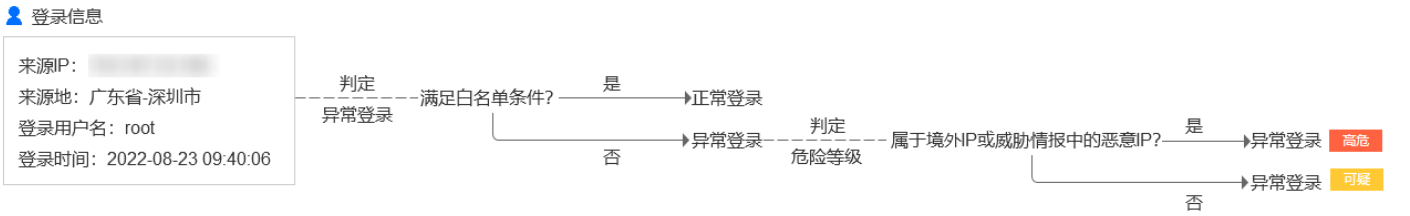
异常登录

最近更新时间: 2024-08-23 15:08:00

本文将为您介绍异常登录的功能和操作。

概述

当检测到存在不满足白名单（常用来源 IP、常用用户名、常用登录地、常用登录时间）的服务器登录行为，将产生异常登录告警。若异常登录来源 IP 属于境外 IP（含中国港澳台地区）或威胁情报中的恶意 IP，将被标记为“高危”，反之则标记为“可疑”。



限制说明

- 已安装主机安全客户端的主机（客户端在线），均会实时监控异常登录行为。
- 主机安全控制台仅保留近6个月的异常登录事件，过期的事件数据将不再展示。

操作指南

1. 登录主机安全控制台。

2. 左侧导航中，选择**入侵检测** > **异常登录**，各功能说明如下。

事件列表

在事件列表页面中，可查看并处理主机安全监测到的异常登录风险。

字段说明：

- 服务器 IP/名称：被异常登录的服务器。
- 来源 IP：登录来源 IP，一般是公司网络出口 IP 或网络代理 IP。
- 来源地：登录来源 IP 所在的地域。
- 登录用户名：成功登录服务器时使用的登录用户名。
- 登录时间：成功登录服务器的时间（服务器上的时区时间）。

- 危险等级：可疑/高危。
- 状态
  - 异常登录：本次登录存在异常地域、异常用户名、异常登录时间或异常来源 IP 登录。
  - 已加入白名单：登录来源 IP 已被添加至白名单（登录源 IP、登录用户名、登录时间、常用登录地、生效范围的组合构成白名单判定规则）。
  - 已处理：用户已手动处理，并将该事件标记为已处理。
  - 已忽略：用户已忽略本次告警事件。
- 操作
  - 处理
    - 标记已处理：若您已人工对该风险事件进行处理，可将事件标记为已处理。
    - 加入白名单：加入白名单操作后，**当再次发生相同事件时将不再进行告警，请谨慎操作。**
    - 忽略：仅将本次告警事件进行忽略，若再有相同事件发生依然会进行告警。
    - 删除记录：删除该事件记录，控制台将不再显示，**无法恢复记录，请慎重操作。**

白名单管理

在白名单管理页面中，可增/删/改/查异常登录的白名单。

字段说明：

- 服务器 IP/名称：该白名单生效的服务器。
- 来源 IP：加白名单的登录来源 IP。
- 常用登录地：加白名单的登录地。
- 登录用户名：加白名单的用户名。
- 登录时间：加白名单的登录时间段。
- 创建时间：该白名单的创建时间。
- 修改时间：最近一次修改白名单的时间。
- 操作
  - 编辑：可重新编辑登录源 IP、登录用户名、登录时间、常用登录地、生效范围等。
  - 删除：可对白名单进行删除操作。

热点问题

收到异常登录告警后该如何处理？

判断该登录行为是否自己操作。

- 若是自己的登录行为，且您不希望再看到告警，请单击**处理**选择**加入白名单**操作，对常见登录源 IP、登录用户名、登录地、登录时间、生效范围进行设置。

登录源 IP 为空：代表所有来源 IP 对服务器进行登录，均不产生告警。 登录用户名为空：代表对服务器的任何用户名进行登录，均不产生告警。 登录地为空：代表不论登录地域在哪，均不产生告警。 登录时间为空：代表不论何时登录，均不产生告警。

> **注意：**
>
> 登录源IP、登录用户名、登录地、登录时间不能同时为空。

- 若不是自己的登录行为，请立即修改服务器登录密码（建议修改为10位以上，包含大小写字母和特殊字符的强密码）。 服务器被异常登录，登录者很有可能已经入侵您的服务器并留下恶意文件。建议您立即进行 文件查杀、漏洞检测、基线检测 以加固您的服务器安全。

白名单怎么设置可以满足大部分用户需求？

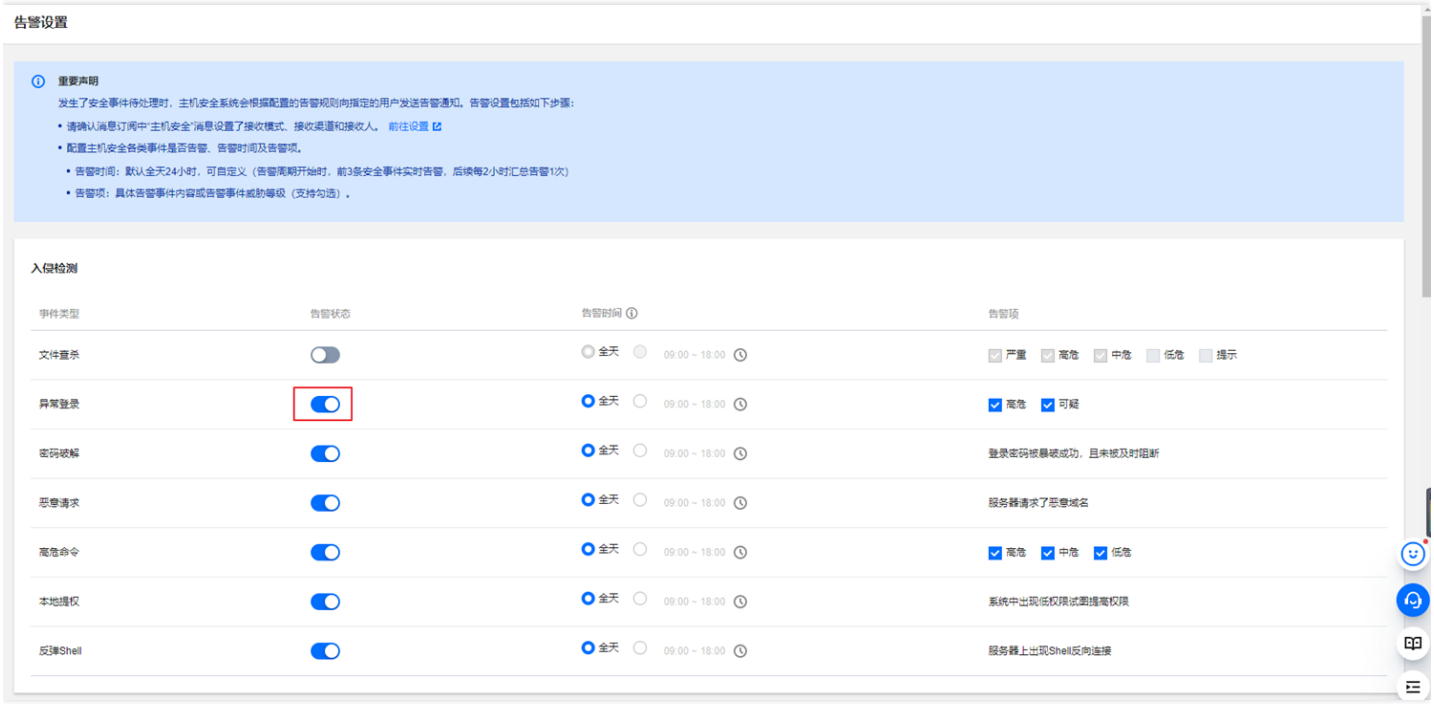
- 场景1：固定 IP 网段登录源可以使用任一用户名对服务器进行登录，而不产生异常登录告警。 您可在登录源 IP 中输入 IP 段，选择生效服务器范围即可。

- 场景2：登录源 IP 是动态变化的，要支持登录地是中国香港地区的 IP 随时都可以使用任一用户名对服务器进行登录，而不产生异常登录告警。 您可在常用登录地中选择香港特别行政区，选择生效服务器范围即可。

> 说明：
>
> 登录条件支持组合。

如何关闭异常登录告警？

请前往 告警设置 对异常登录的告警开关进行关闭。若保持告警开关开启，建议勾选高危选项，仅告警高危的异常登录行为即可。



密码破解

最近更新时间: 2024-08-23 15:08:00

主机安全的 密码破解 基于网络安全防御和主机入侵检测能力，为主机提供密码暴力破解行为实时监控，实现自动阻断防御功能。

全局阻断设置

前提条件

“对全局阻断进行设置”功能仅专业版主机支持，基础版和未防护主机须 升级专业版 才可使用该功能。

操作指南

通过设置全局阻断规则与阻断模式，实现自动阻断防御功能，操作步骤如下：

1. 登录主机安全控制台，在左侧导航中，选择**入侵检测** > **密码破解**，进入密码破解页面。

   开启自动阻断开关。在密码破解页面上方，用户可一键开启自动阻断开关。

2. 设置阻断模式。在阻断模式右侧单击**设置**，弹出设置页面，在设置页面进行相关设置，设置完成后，单击**确定**即可，字段说明如下：
   - **判断暴破规则**：支持用户自定义“判断暴破规则”，最多支持添加5条。

- **阻断模式**：密码破解共提供两种阻断模式。
  - **标准阻断（默认推荐）**：设置“暴破规则”智能识别暴破行为，过滤白名单来源 IP，针对暴破来源 IP 自动阻断。
  - **深度阻断（请谨慎选择）**：设置“白名单-非白即黑”策略，非白名单的来源 IP 将自动阻断（仅支持22、3389端口）。

> 注意：
>
> 深度阻断兼容标准阻断，例：某非白名单的来源 IP 通过55端口登录，即便不是22、3389端口，但因命中了标准阻断规则，仍将被阻断。
>
> 请慎重选择深度阻断，需要用户配置完善的白名单，避免误阻断。若出现误阻断情况，您可通过“加白名单”或“关闭自动阻断”来解除阻断，数据同步5分钟内生效。

- **阻断区域**：表示阻断功能可支持的用户服务器所在区域。

配置白名单

配置白名单后，属于白名单来源 IP 的密码破解行为将不会被阻断与告警，操作步骤如下：

1. 登录主机安全控制台，在左侧导航中，选择**入侵检测** > **密码破解**，进入密码破解页面。

2. 在密码破解页面，单击**白名单管理**，进入白名单管理页面。

3. 在白名单管理页面，单击添加白名单，进入创建白名单页面中。

4. 在新增白名单页面中，填写来源 IP 及生效范围。

> **注意：**
>
> - 添加白名单后，该来源 IP 的密码破解行为将不会被阻断与告警，请慎重操作。若有非白名单来源 IP 尝试登录，并命中暴力破解规则时，系统将自动发出异常告警或阻断。
> - 当来源 IP 为腾讯云内网 IP 时，不论有没有加入白名单，均不发生阻断。

参数说明：

- 来源 IP：支持填写单个 IP、IP 范围（如1.1.1.1-1.1.1.10）或 IP 段（如1.1.1.0/24）。
- 生效范围：
  - 全部服务器（**请谨慎选择**）：将对用户 AppID 下所有服务器添加信任该白名单条件。
  - 自定义服务器范围：自定义选择添加信任该白名单条件的服务器范围。
- 备注：建议您输入相关规则备注。

查看密码破解事件

登录主机安全控制台，在左侧导航中，选择**入侵检测** > **密码破解**，进入密码破解页面，所有暴力破解事件将会在暴力破解列表中展示。

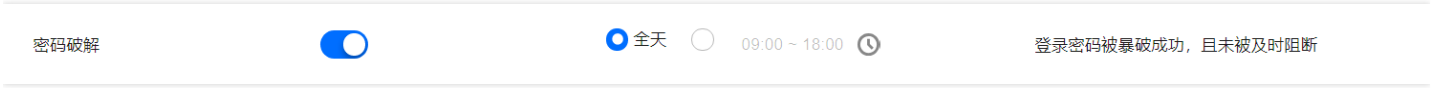
字段说明：

- 服务器 IP/名称 ：当前被暴力破解的服务器。
- 来源 IP：攻击来源 IP 地址。
- 来源地：攻击来源 IP 所在地域。
- 协议：攻击者通过的协议，含 ssh/rdp、ftp、mssql、mysql、smb、mongodb、kafka、rabbitmq。
- 登录用户名：攻击者登录使用的用户名。
- 端口：攻击者登录使用的端口。

- 首次攻击时间：主机安全首次监控到密码破解行为的时间。
- 最近攻击时间：该事件最近再次发生的时间。
- 攻击时间：攻击者发起暴力破解时间。
- 尝试次数：攻击 IP 尝试暴力破解的次数统计。
- 破解状态：当前服务器被暴力破解成功或失败说明。
- 阻断状态：针对本次攻击的自动阻断成功或未阻断说明。
- 操作：
  - 升级版本：当前服务器为升级为专业版主机安全，可单击**升级版本**进行升级。
  - 加入白名单：当出现错误阻断时，可以单击**加入白名单**立即解除阻断。
  - 删除记录：支持删除该事件，删除记录后将不再显示该记录。

开启告警通知

登录主机安全控制台，在左侧导航中，选择**设置中心** > **告警设置**，在告警设置中，开启告警通知开关，当前产生密码破解事件时，会以站内信、短信、邮件、微信及企业微信进行通知。



密码破解事件处置指引

1. 当用户接收密码破解事件告警时，登录主机安全控制台，在左侧导航中，选择**入侵检测** > **密码破解**，进入密码破解页面。

2. 查看告警事件列表中的对应攻击来源 IP。

   若确认是可信来源 IP，用户需在该事件右侧操作栏中，单击**处理** > **加入白名单**，设置加白名单条件和生效范围（**请用户谨慎添加白名单**）。配置成功后，预计5分钟内生效，后续来自该来源 IP 的密码破解行为将不再进行告警或者阻断。

- 若确认是不可信来源 IP，且服务器已被攻击者密码破解成功。

  i. 首先确认当前服务器的主机安全是否已升级为专业版，若未升级为专业版，建议用户在该事件右侧操作栏中，单击**升级版本**，升级为专业版主机安全。

2. 在密码破解页面上方，开启自动阻断开关，**推荐选择标准阻断**模式，后续来自该攻击来源 IP 将会自动阻断，默认阻断时长15分钟，用户可根据需要自定义时长。

3. 针对已被密码破解入侵的服务器，建议用户立即重新设置复杂密码（大写+小写+特殊字符+数字组成的12-16位的复杂密码），并检查账号列表中是否存在陌生账号，若存在陌生账号，需将陌生账号删除或者禁用，同时排查系统异常情况。

本地提权

最近更新时间: 2024-08-23 15:08:00

本文档将为您介绍如何对提权事件详情进行查看和处理，同时指导您如何创建白名单，用于设置被允许的提权行为。

背景信息

若出现以低权限进入系统，通过某些手段提升权限，获取到高权限的事件，很有可能为黑客的攻击行为，该行为会危害到主机安全。本地提权功能可实时监控您云服务器上的提权事件，并能对提权事件详情进行查看和处理，同时也支持白名单创建功能，用于设置被允许的提权行为。

前提条件

本地提权功能仅专业版主机主机支持，基础版和未防护主机须 升级专业版 才可使用该功能。

操作步骤

事件列表

1. 登录主机安全控制台，在左侧导航栏，选择**入侵检测** > **本地提权**，进入本地提权的事件列表标签页。

2. 在本地提权的"事件列表"标签页，可查看本地提权事件列表，并进行相关操作。 在**事件列表**标签页，可查看发生提权事件的服务器 IP/名称、提权用户、发现时间、状态、操作（详情、加入白名单及删除记录）等12个字段，展示列表详情信息可进行自定义。
   - **筛选事件**：本地提权事件列表支持选择日期查看相应的事件，支持按关键字及标签查询（多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔）事件，同时支持按状态、筛选事件。

- **自定义设置列表字段**：在本地提权事件列表上方，单击，可设置列表展示字段，选择完成后，单击**确定**，即可设置成功。

- **事件导出**：在本地提权事件列表上方，单击 ，可将本地提权事件列表导出。
- **详情**：在本地提权事件的右侧操作栏，单击**详情**，可查看本地提权事件详情。

- **加入白名单**：如需将本地提权事件加入白名单，可在目标本地提权事件的右侧操作栏，单击**加入白名单**，确认无误后，在弹窗中，单击**提交**，即可将该本地提权事件加入白名单事件。
- **删除记录**：本地提权事件列表支持对本地提权事件进行删除。

3. 单击本地提权事件的服务器 IP，可查看该服务器详情。

白名单管理

本地提权功能支持添加白名单，通过设置白名单提权条件，将满足条件的事件标记为白名单。

1. 登录主机安全控制台，在左侧导航栏，选择**入侵检测** > **本地提权**，进入本地提权页面。

2. 在**本地提权**页面，选择**白名单管理** > **添加白名单**。

3. 在**添加白名单**页面，设置提权条件，包括：带 S 权限的进程、自定义提权进程（支持多个进程名，以英文逗号分隔，例如 123.exe,test.exe），同时选择该条件覆盖的服务器范围，单击**确定**。

> **注意：**
>
> - s 权限： 设置使文件在执行阶段具有文件所有者的权限，相当于临时拥有文件所有者的身份。
> - 勾选两个条件时，需要同时满足才能命中白名单。
> - 若服务器范围选择全部服务器，将对用户 APPID 下所有服务器添加信任该白名单条件，请谨慎操作。

4. 设置完成后，可在白名单管理列表查看该条件，且在事件列表满足该条件的事件即会被标记为白名单事件。

5. 在白名单管理页面，可对白名单进行筛选删除等操作。

   - **筛选**：已配置的白名单支持按关键字及标签查询（多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔）筛选，同时支持按是否带 S 权限进行筛选。

- **自定义设置列表字段**：在白名单列表上方，可设置列表展示字段，选择完成后，单击**确定**，即可设置成功。

- **编辑**：在目标白名单的右侧操作栏，单击**编辑**，可对已创建的白名单进行编辑。

- **删除**：在白名单列表中，支持对已配置的白名单进行删除。


添加白名单
删除
多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔
服务器
提权进程
是否带S权限
创建时间
更新时间
操作
全部服务器
全部进程
是
2020-11-25 23:10:49
2020-11-25 23:10:49
编辑
删除
全部服务器
全部进程
是
2020-11-20 15:12:17
2020-11-20 15:12:17
编辑
删除

反弹Shell

最近更新时间: 2024-08-23 15:08:00

本文档将为您介绍如何对反弹 Shell 详情进行查看和处理，同时指导您如何创建白名单，用于设置被允许的反向连接行为。

背景信息

反弹 Shell 功能是基于尚航云_V1安全技术及多维度多手段，对服务器上的 Shell 反向连接行为进行识别记录，为您的云服务器提供反弹 Shell 行为的实时监控能力。

前提条件

反弹 Shell 功能仅专业版主机支持，基础版和未防护主机须 升级专业版 才可使用该功能。

操作步骤

事件列表

1. 登录主机安全控制台，在左侧导航栏，选择**入侵检测** > **反弹 Shell**，进入反弹 Shell 的事件列表标签页面。

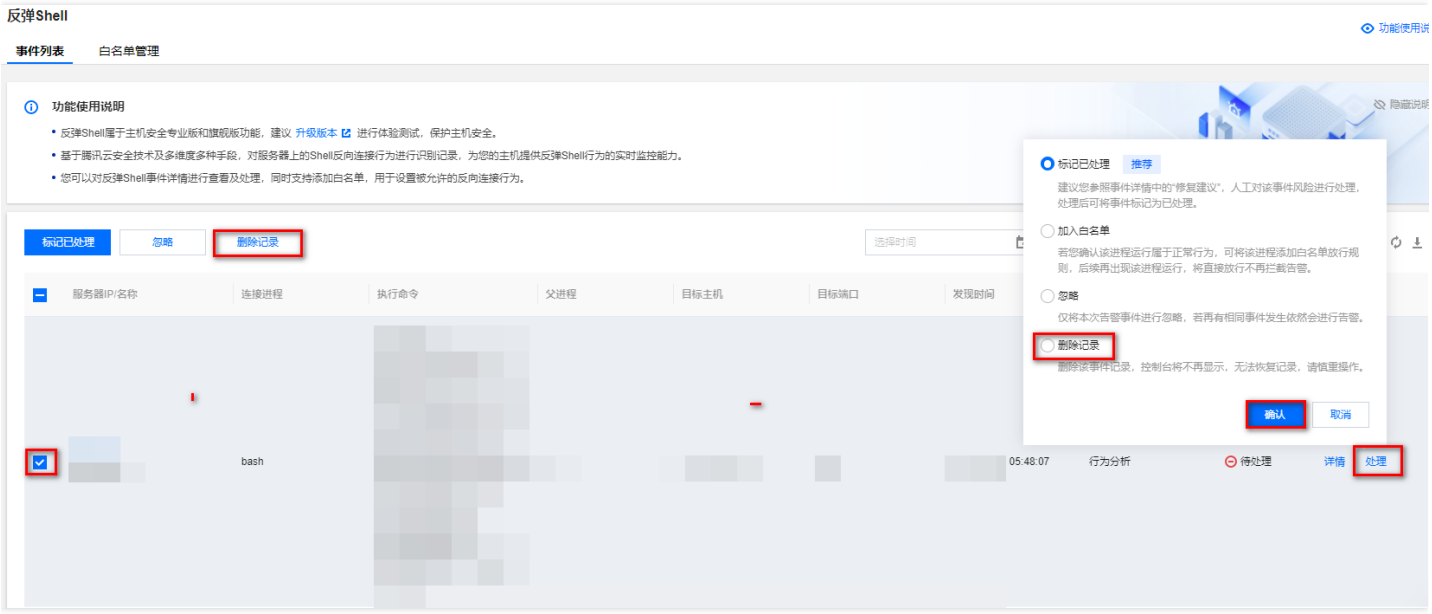
2. 在反弹 Shell 的"事件列表"标签页面，可查看反弹 Shell 事件列表，并进行相关操作。 在事件列表标签界面，可查看发生反弹 Shell 的服务器 IP/名称、连接进程、发现时间、状态（全部、待处理及加入白名单），操作（详情、加入白名单及删除记录）等12个字段，展示列表详情信息可进行自定义。
   - **筛选事件**：反弹 Shell 事件列表支持选择日期查看相应事件，支持按关键字及标签查询（多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔）事件，同时支持按状态（全部、待处理及已确认）筛选事件。

- **自定义设置列表字段**：在反弹 Shell 事件列表上方，单击 ，可设置列表展示字段，选择完成后，单击**确定**，即可设置成功。

- **事件导出**：在反弹 Shell 事件列表上方，单击 ，可将反弹 Shell 事件列表导出。

- **详情**：在目标反弹 Shell 事件的右侧操作栏，单击**详情**，可查看反弹 Shell 事件详情。

- **加入白名单**：如需将反弹 Shell 事件加入白名单，可在目标反弹 Shell 事件的右侧操作栏，单击**处理** > **加入白名单**，确认无误后，在弹窗中，单击**提交**，即可将该反弹 Shell 事件标记为白名单事件。
- **删除记录**：反弹 Shell 事件列表支持对反弹 Shell 事件进行删除。



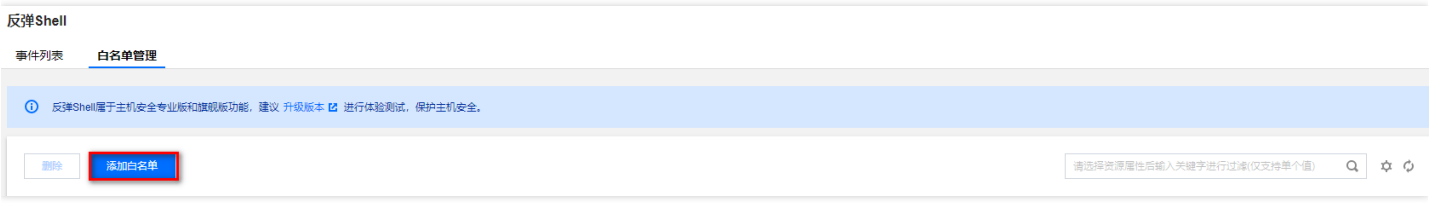
3. 单击反弹 Shell 事件的服务器 IP，可查看该服务器详情。

白名单管理

反弹 Shell 功能支持添加白名单，通过设置白名单条件，将满足条件的事件标记为白名单。

1. 登录主机安全控制台，在左侧导航栏，选择**入侵检测** > **反弹 Shell**，进入反弹 Shell 页面。

2. 在"反弹 Shell "页面，选择白名单管理 > 添加白名单。



3. 在"添加白名单"页面，设置反弹 Shell 条件，包括：目标主机、自定义连接进程（支持多个进程名，以英文逗号分隔），同时选择该条件覆盖的服务器范围，单击确定。

参数说明：

- IP 地址格式：单个 IP（127.0.0.1）、IP 范围（127.0.0.1-127.0.0.254）、IP 网段（127.0.0.1/24）。
- 端口格式：80,8080（支持多个端口并以英文逗号分隔，不限端口请留空）。
- 勾选两个条件时，需要同时满足才能命中白名单。
- 若服务器范围选择全部服务器，将对用户 APPID 下所有服务器添加信任该白名单条件，请谨慎操作。

4. 设置完成后，可在白名单管理列表查看该条件，且在事件列表满足该条件的事件即会被标记为白名单事件。

5. 在白名单管理页面，可对白名单进行筛选删除等操作。
   - **筛选**：已配置的白名单支持按关键字及标签查询（多个关键字用竖线 "|" 分隔，多个过滤标签用回车键分隔）筛选。

- **自定义设置列表字段**：在白名单列表上方，单击 ，可设置列表展示字段，选择完成后，单击**确定**，即可设置成功。

- **编辑**：在目标白名单的右侧操作栏，单击**编辑**，可对已创建的白名单进行编辑。

- **删除**：在白名单列表中，支持对已配置的白名单进行删除。

高危命令

最近更新时间: 2024-08-23 15:08:00

本文档将为您介绍如何查看并操作高危命令事件列表。

背景信息

基于尚航云_V1安全技术及多维度多种手段，主机安全可对系统中的命令实现实时监控，并且可通过配置规则对命令危险程度进行等级划分，若检测出高危命令，系统会向您提供实时告警通知。

前提条件

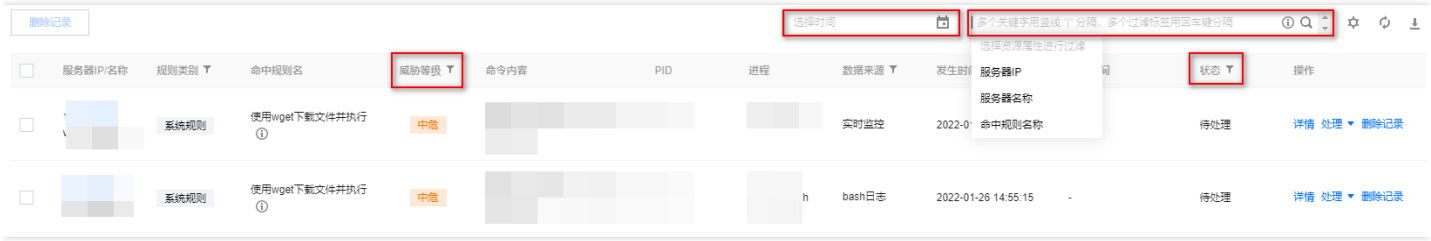
高危命令功能仅专业版主机支持，基础版和未防护主机须 升级专业版 才可使用该功能。

操作步骤

事件列表

1. 登录主机安全控制台，在左侧导航栏，选择**入侵检测** > **高危命令**，进入高危命令的事件列表标签页。

2. 在高危命令的**事件列表**标签页，可查看高危命令事件列表，并进行相关操作。在事件列表界面可展示发生高危命令事件的服务器IP/名称、规则类别、命中规则名、威胁等级、命令内容、数据来源、发生时间、处理时间、状态及操作等12个字段，展示列表字段可进行自定义。
   - **筛选事件**：高危命令事件列表支持选择日期查看相应的事件，支持按关键字及标签查询（多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔）事件，同时支持按威胁等级及状态筛选事件。



- **自定义列表字段**：在高危命令事件列表上方，单击 ，可设置列表展示字段，选择完成后，单击**确定**，即可设置成功。

- **事件列表导出**：在高危命令事件列表上方，单击 ，可将高危命令事件列表导出。
- **详情**：单击**详情**，可查看高危命令事件详情及进程树信息。

- **加入白名单**：单击**处理** > **加入白名单**，可对信任的命令加入白名单，后续该命令再被执行将不再产生告警。

> 说明：
>
> 针对本高危命令事件的命令，单击自动生成可支持自动生成正则表达式，也可以对符合本白名单的历史待处理事件执行加白操作。

- **已手动处理**：若用户已手动处理了本次高危命令事件，可将该事件标记为已手动处理，便于维护。
- **删除记录**：支持单选&多选高危命令事件，对事件记录进行删除，删除后将不再显示。

用户规则配置

高危命令功能支持新增规则，通过设置规则对满足条件的事件进行标记危险等级。

1. 登录主机安全控制台，在左侧导航栏，选择**入侵检测** > **高危命令**，进入高危命令页面。

2. 在高危命令页面，选择用户规则配置 > 新增规则。

3. 在新增规则页面，选择规则类别（黑名单/白名单），填写规则名称和正则表达式，选择生效服务器范围，支持勾选历史事件自动加白。
   - 黑名单规则，指命令内容一旦命中黑名单的正则表达式，则将产生安全事件告警。

- 白名单规则，主要是为部分误告警的服务器提供加白操作。

> 注意：
>
> - 若服务器范围选择全部服务器，将对用户 APPID 下所有服务器添加信任该白名单条件，请谨慎操作。
> - 检测到系统命令字符串匹配正则表达式，即视为高危命令（正则表达式也可为某具体命令）。

4. 设置完成后，可在用户规则配置列表查看该规则，在事件列表中满足黑名单规则的事件即会被标记为相应的威胁等级。

5. 在用户规则配置页面，可对规则进行筛选删除等操作。

字段说明：

- **筛选**：已配置的用户规则支持按关键字及标签查询（多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔）筛选，同时支持按威胁等级（全部、高、中及低）进行筛选。

- **自定义设置列表字段**：在规则列表上方，单击 ，可设置列表展示字段，选择完成后，单击**确定**，即可设置成功。
- **编辑**：在规则列表的右侧操作栏，单击**编辑**，可对已创建的规则进行编辑。
- **删除**：在规则列表中，支持对已配置的规则进行删除。
- **启用状态**：在规则列表中，支持设置规则的启用状态，可在启用状态列，单击启用开关，决定该规则是否启用。

漏洞管理

最近更新时间: 2024-08-23 15:08:00

本文将为您介绍漏洞管理的功能和操作，帮助您管理服务器中的漏洞风险。

概述

云平台主机安全支持对目前主流主机（Windows，Linux 等）上的漏洞进行周期性和及时性检测。主机安全支持对指定主机和漏洞类别进行检测，同时支持忽略漏洞等功能，可为您提供漏洞的风险、特征、严重等级及修复建议等信息，可视化界面有助于您更好地管理服务器中的漏洞风险。

限制说明

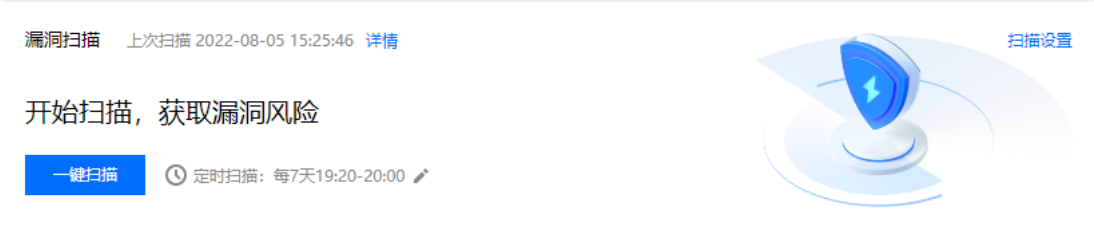
- 至少存在1台已绑定防护授权的主机（**专业版**），才可解锁漏洞管理功能。
- 漏洞防御功能仅支持专业版主机。
- 支持检测的漏洞：Linux 软件漏洞、Windows系统漏洞、Web-CMS 漏洞、应用漏洞。
- 支持自动修复的漏洞：Linux 软件漏洞（部分）、Web-CMS 漏洞（部分）。

操作指南

1. 登录主机安全控制台 。
2. 单击左侧导航中的**漏洞管理**，各功能说明如下。

漏洞扫描

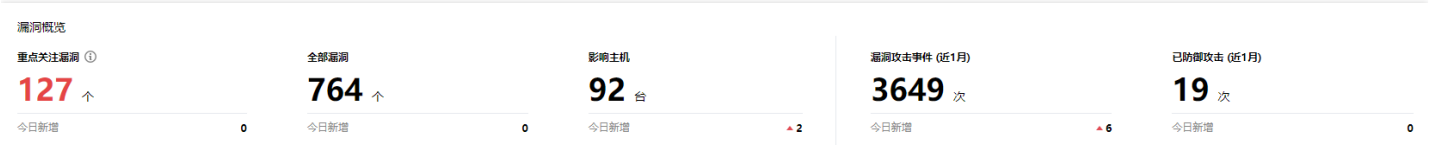
在**漏洞扫描**区域中，您可进行一键扫描，获取漏洞扫描的结果，也可设置定时扫描，及时暴露漏洞风险并进行处理。



- 单击**一键扫描**将打开**一键扫描设置**弹窗，您可对本次扫描的漏洞类别、漏洞等级、扫描超时时长、扫描服务器范围进行设置，设置后可立即扫描。
- 单击**扫描设置**或**定时扫描**的编辑图标，可打开**漏洞设置**弹窗并锚点至**定时扫描**，您可对定时扫描开关、定时扫描周期、漏洞等级及漏洞类别进行设置，设置后可立即应用。
- 单击**详情**可查看上一次扫描的详情，并支持下载 PDF 扫描报告、Excel 扫描结果。

漏洞概览

在**漏洞概览**区域中，展示了漏洞检出、漏洞防御（旗舰版功能）两个维度的数据统计及今日新增情况。



- 重点关注漏洞：检出重点关注漏洞（即对外暴露、严重/高危的漏洞）的数量。
- 全部漏洞：检出 Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞的数量总和。
- 影响主机：检出漏洞的主机数量。
- 漏洞攻击事件：统计近1个月内 WeDetect 网络攻击事件的数量。（旗舰版功能）
- 已防御攻击：统计近1个月内防御攻击事件的数量。（旗舰版功能）

漏洞列表

在**漏洞列表**区域中，已分为应急漏洞、重点关注漏洞、全部漏洞3类，由于均属于漏洞检出维度，功能无太大差异，下面以**全部漏洞**举例，为您介绍漏洞列表的功能操作。

漏洞列表各字段说明：

- 漏洞名称/标签：漏洞名称指当前检出的漏洞，标签指该漏洞的标签（如：远程利用、服务重启、存在 EXP 等）。
- 漏洞类型：Linux 软件漏洞、Windows 系统漏洞、Web-CMS 漏洞、应用漏洞。
- 威胁等级：严重、高危、中危、低危。
- CVSS：指通用漏洞评分系统的评分，分数范围从0到10，0代表最不严重，10代表最严重。
- CVE编号：公共漏洞暴露库中，识别该漏洞的唯一编号。
- 最后扫描时间：最近一次扫描到该漏洞的时间。
- 影响主机：存在该漏洞的主机数量。
- 处理状态：待修复、修复中、扫描中、已修复、已忽略、修复失败。
- 防御状态：防御中、空（暂不支持防御）。
- 操作
  - 修复方案：暂不支持自动修复的漏洞，可单击**修复方案**打开漏洞详情弹窗，根据修复方案手动修复漏洞。
  - 重新扫描：重新对该漏洞进行扫描。
  - 忽略：对该漏洞进行忽略，后续不再对该主机扫描该漏洞。

基线管理

最近更新时间: 2024-08-23 15:08:00

本文档将介绍如何使用基线管理功能，帮助您管理服务器中的基线安全。

背景信息

云平台主机安全支持对基线检测项进行定期检测和一键检测，支持对指定主机上的指定基线项进行检测，支持通过检测策略了解基线通过率及风险情况，提供基线和检测项的风险等级和修复建议，提供尚航云_V1默认基线策略，有助于您更好的管理服务器中的基线安全。

主机安全版本

- **基础版**：首次使用时，支持对默认策略内的全量主机进行检测，只展示5条结果。不支持对基线策略的管理、对策略的一键检测及周期检测。
- **专业版**：支持基线策略的管理，支持用户自己新建或编辑策略，支持对基线策略的周期检测与一键检测功能。

操作指南

1. 登录主机安全控制台，在左侧导航栏中，选择**基线管理** > **安全基线**，进入安全基线页面。
2. 在安全基线页面提供基线策略的设置、周期性检测和指定策略的一键检测功能，支持查看基线策略的通过率和风险状况，以及基线检测结果列表，并可查看基线和检测项详情信息及修复方案，可对指定服务器检测项进行忽略。

基线策略

基线策略是基于用户自定义设置的基线检测项的集合，基于策略维度了解基线的通过率及风险情况。

- **云平台默认基线策略**：云平台主机安全根据网络安全主流的基线检测内容为您提供默认基线检测策略，包括：等保二级策略、等保三级策略、弱密码策略、CIS 基线策略、云平台最佳安全实践策略。您可以增加默认基线策略中的检测项和需要检测的服务器，该策略默认每隔7天，第7天晚上0点检测全量专业版服务器。

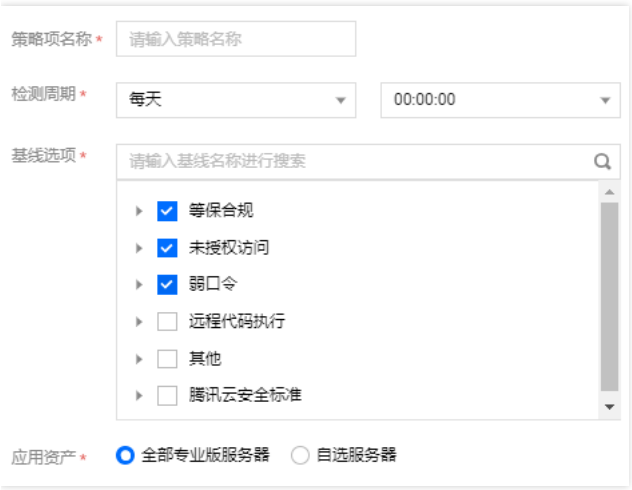
> **说明：**
>
> 策略的通过率 = 已通过该策略下全部检测项的服务器数 / 该策略下全部检测的服务器数

- **新增基线策略**

1. 在基线检测结果展示模块右上角，单击**基线设置**。
2. 在设置页面的基线策略设置页面，单击新增策略。

3. 在新增基线策略页面，输入策略项名称（不允许与现存策略名称重复）、选择检测周期、基线选项及应用资产，单击保存并更新。

> 说明：
>
> - 主机安全最多支持创建20个基线策略，达到20个后则不允许再创建，但您可以删除现有基线后，再次创建。
> - 云平台默认策略会存在"系统策略"标签内。



基线检测

云平台主机安全支持对基线检测项的**定期检测**和**一键检测**，支持对指定云服务器上的指定基线项进行检测。

> 说明：
>
> 若非首次基线检测，需开通 主机安全专业版 才可进行基线检测。

- **一键检测**
  - **首次检测**：当您首次使用基线检测功能时，我们为您免费提供一次全量基线策略和全服务器的检测服务，协助您发现基线安全风险，并展示其中5条基线风险。若您所需更多的基线安全功能，建议 升级专业版。

    基线检测结果展示模块，单击**试用检测**。

a.在"检测提示"弹窗中：

- 操作1：选择需要检测的基线策略，单击**开始检测**（检测一般持续2 - 5分钟），检测完成后，检测结果会以可视化图表的方式显示在漏洞管理页面。

- 操作2：单击[立即升级](http://buy.cloud.sunhongs.com/yunjing?ADTAG=cwp.buy.pro.vulManage)，跳转至主机安全升级界面，将云服务器升级为专业版。

- **非首次检测**：当您非首次使用基线检测时，选择需要检测的基线策略后，单击**一键检测**（检测一般持续2 - 10分钟）若您尚未存在专业版服务器，建议立即 升级专业版。

- **周期检测**

1. 基线检测结果展示模块右上角，单击基线设置。

2. 在基线策略设置页签，可以进行周期检测设置并进行忽略检测项管理。

   - **周期检测设置**：在"设置"弹窗中的"基线策略设置"标签内，您可以新建或编辑策略，设置检测周期，同时可以开启或关闭定期检测策略，支持对用户自定义策略的删除。

- **忽略检测项管理**：在"设置"弹窗中的"忽略检测项管理"标签内，查看已忽略的检测项及其详情，并可进行取消忽略操作。

基线数据可视化

当您选择基线策略并检测完成后，您可以在 安全基线 页面，查看本次检测服务器的数量、检测项数量、该基线策略的通过率、基线检测项 TOP5 及服务器风险 TOP5，并按照威胁等级来进行划分。

基线结构列表

在 安全基线 页面下方，可查看基线检测结果列表，支持查看基线详情，支持对单个基线进行模糊搜索和状态筛选，并支持对所有表格进行下载。

字段说明：

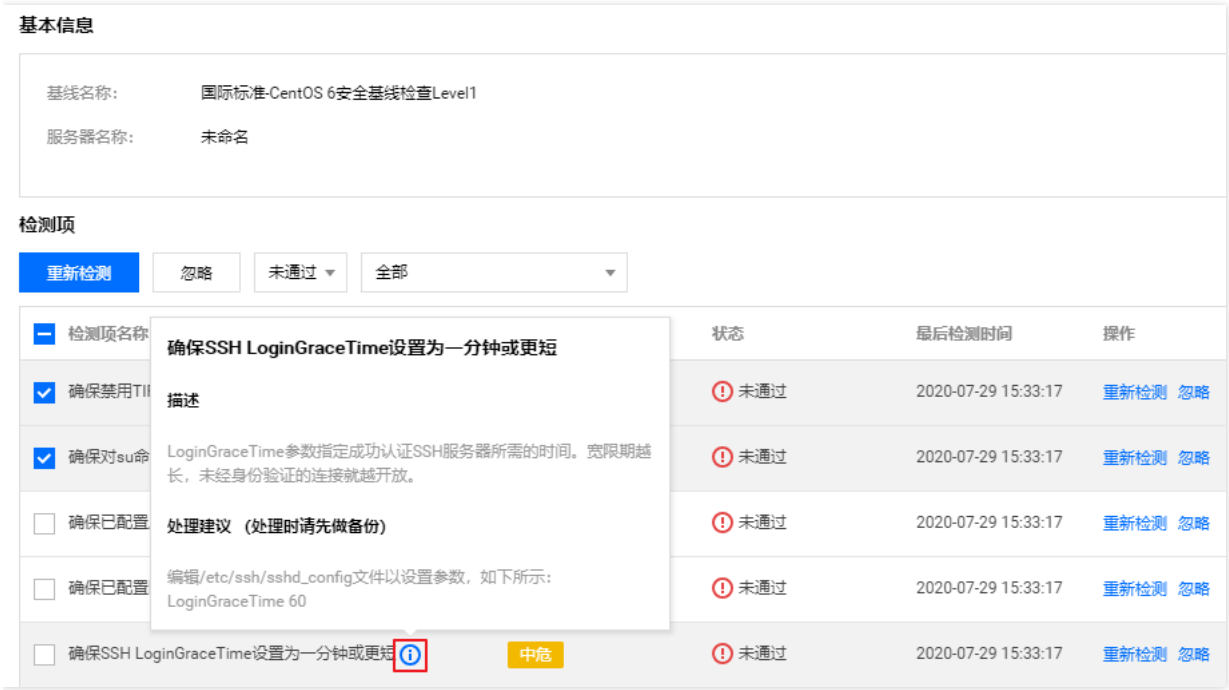
- **基线名称**：基线包名称，包含若干相同类别的检测项。
- **威胁等级**：根据基线的危险程度，将其划分为严重、高危、中危和低危四个等级。
- **基线检测项**：该基线包下所有的检测项合计数量。

- **影响服务器数**：表示在该策略所选服务器和检测项下，被检测服务器未全部通过该基线包下的检测项数量，即该基线包影响服务器的数量。
- **最后检测时间**：取最近一次某台服务器检测出该基线包下的检测项的时间。
- **处理状态**：分为“已通过”、“未通过”、 “检测中”
- **操作**：支持查看基线详情并对未通过检测的基线重新检测。
  - **重新检测**：
    - 方式1：选择需要检测的基线，在列表左上角单击**重新检测**，将批量对基线进行重新检测。
    - 方式2：在目标基线右侧，单击**重新检测**，将重新对该基线进行检测。
  - **查看详情**：

    a.在基线检测结果列表中，找到目标基线，在右侧操作栏，单击**查看详情**，进入基线详情页。

    b.在基线详情页面，可查看该基线的描述信息和威胁等级，同时可查看影响服务器的列表。 服务器列表支持对单个服务器模糊搜索、支持状态筛选、支持批量对服务器进行“重新检测”、支持查看单个服务器详情，在目 标服务器右侧操作栏，单击**详情**，进入检测详情页。

c.在检测详情页可查看基本信息，包括基线名称、服务器名称和检测项详情列表。



- 列表支持对多个检测项“重新检测”和“忽略”，忽略后的检测项可进入 “忽略风险项管理” 页面进行查看。

- 支持对检测项的威胁等级筛选和处理状态筛选。

- 鼠标停留在检测项时，为您提供该检测项的详细描述和处理建议。

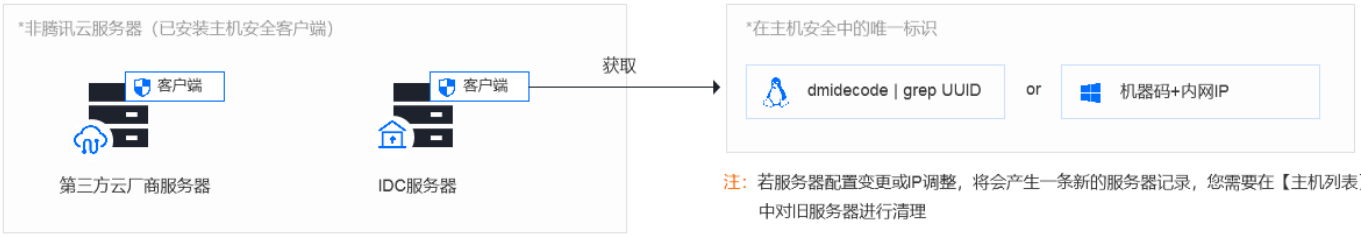
混合云安装指引

概述

最近更新时间: 2024-08-23 15:08:00

背景信息

随着企业上云率提升，更多中大型企业选择公有云+私有云的混合云模式，兼具公有云成本低、敏捷、灵活、使用方便及私有云可控、安全、高可用部署的优点。混合云管理功能能够支持用户接入非云平台机器，更好地帮助用户统一管理和监控主机安全。



功能概述

- 支持云平台的边缘计算机器、轻量应用服务器自动接入主机安全。
- 支持非云平台服务器，如：私有云、阿里云、华为云、青云、亚马逊云、UCloud 等云服务器手动接入主机安全。

客户端支持版本说明

Linux 系统支持版本

- RHEL：Versions 6 .1+（64 bit）
- CentOS：Versions 6.3+（64 bit）
- Ubuntu：9.10+（64 bit）
- Debian：6+（64 bit）

Windows 系统支持版本

- Windows server 2012，2016，2019
- Windows server 2008+ R2
- Windows server 2003（limited support）

配置非腾讯云机器

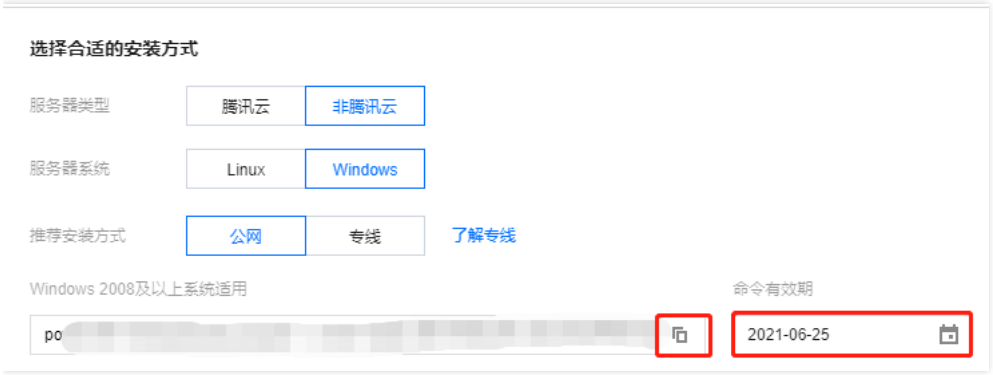
最近更新时间: 2024-08-23 15:08:00

步骤1：安装主机安全客户端

1. 登录主机安全控制台，在左侧导航栏，单击**资产管理** > **主机列表** > **安装主机安全客户端**，在右侧弹窗中查看安装指引详情。

2. 在安装指引中选择服务器类型、服务器系统及推荐安装方式，如果是通过专线打通云上云外的话，选择专线安装方式，否则选择公网的安装方式。

- 通过公网接入：单击 图标复制并执行相应命令，即可安装主机安全客户端，**需注意命令有效期。**



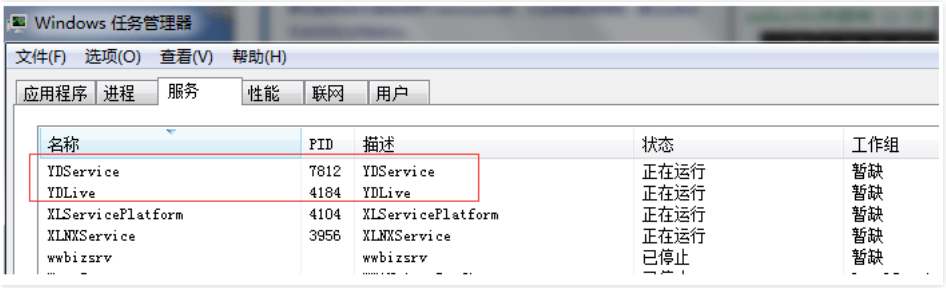
- 通过专线接入：选择已连专线的 VPC，单击 图标复制并执行相应命令，即可安装主机安全客户端，**需注意命令有效期。**

> **说明：**
>
> - 如需了解专线相关，可单击了解专线跳转专线接入控制台。
> - 如防火墙需开放目标 IP，参考图片中④对命令中 IP 开放访问权限。

步骤2：确认是否安装成功

1. 按照安装指引-判断是否安装成功的命令执行，打开任务管理器确认 YDLive 进程有运行，即安装成功。

执行命令： `ps -ef | grep YD` 查看 YDService，YDLive 进程是否有运行。



- 进程无运行，root 用户可手动启动程序，执行命令： /usr/local/qcloud/YunJing/YDEyes/YDService。

```
[root@VM_90_131_centos conf]# ps -ef|grep YD
root     16216 21992  0 14:33 pts/3    00:00:00 grep --color=auto YD
root     32707     1  0 11:23 ?        00:00:09 /usr/local/qcloud/YunJing/YDEyes/YDService
root     32724     1  0 11:23 ?        00:00:01 /usr/local/qcloud/YunJing/YDLive/YDLive
[root@VM_90_131_centos conf]# ps -ef|grep YD
```

2. 安装成功后在 主机列表 页面，单击选择**云服务器专区** > **非云平台服务器专区**，即可查看对应服务器。

> 说明：
>
> - 检查服务是否上线，先检查客户端是否安装成功，然后在主机列表可查看，服务器属"防护中"即服务已上线。
> - 如未正常上线，请联系我们获得支持。

步骤3：升级主机安全版本

单击选择**非云平台服务器专区**，即可查看对应服务器，单击**授权管理**即可进入授权管理页面升级为主机安全**专业版。**

1. 升级后可测试主机安全专业版功能，支持功能包括：资产同步、木马扫描、漏洞扫描、异常登录、密码破解（非尚航云_V1环境不支持阻断）、反弹 shell、本地提权、高危命令、恶意请求等。

连接专线VPC

最近更新时间: 2024-08-23 15:08:00

背景信息

目前 VPC 专线接入暂时只支持华南地区（广州）、华北地区（北京）、华东地区（上海、上海金融、南京），西南地区（成都），已经支持公有云与客户机房网络在VPC内互通，可以直接安装客户端。

操作指南

步骤1：确认是否需要通过云联网进行接入

1.登录主机安全控制台，在左侧导航栏，单击**资产管理** > **主机列表** > **安装主机安全客户端**，在右侧弹窗中查看安装指引详情。

2.在安装指引中，服务器类型单击选择**非尚航云_V1**，**推荐安装方式单击选择专线。**

> 说明：
>
> 服务器系统按照用户的操作系统，选择相对应 Linux 或 Windows 操作系统。

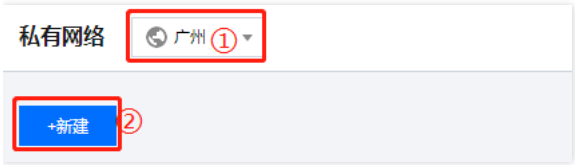
3.如您在华南地区（广州）、华北地区（北京）、华东地区（上海）、华东地区（上海金融）、华东地区（南京）和西南地区（成都）地区：

- 已有和非云平台机房网络互联的 VPC，则选择已连接专线的 VPC 网络，直接使用安装命令安装。
- 没有找到相应的 VPC 网络与您的非云平台机房网络进行互联，可参考步骤2云联网。

步骤2：确认用于连接专线的私有网络

1. 如您在当前华南地区（广州）、华北地区（北京）、华东地区（上海）、华东地区（上海金融）、华东地区（南京）和西南地区（成都）地区没有 VPC 网络，则登录 私有网络 控制台，单击**私有网络**进入私有网络页面。

   在私有网络页面中，单击"下拉框"选择所需区域，单击 **+新建**，弹出新建 VPC 弹窗。



2. 在新建 VPC 弹窗中，输入所需参数单击**确定**，即可完成新建 VPC。

步骤3：通过云联网实现VPC和已连专线的非云平台机房网络互通

1.如已存在和非云平台机房通信的云联网，则将步骤2中选择的 VPC 实例添加到云联网中。 a. 登录 私有网络 控制台，在左侧导航栏，单击**云联网**，进入云联网页面。
b. 在云联网页面，单击右侧**管理实例**>**关联实例**，进入关联实例页面。 c. 在关联实例页面，单击**新增实例**，将步骤2中选择的 VPC 实例添加到云联网中，单击**确定**即完成关联实例。

2.如尚未配置云联网，则需要新建。 a. 登录 私有网络 控制台，在左侧导航栏，单击**云联网**，进入云联网页面。
b. 在云联网页面中，单击**+新建**，弹出新建云联网实例弹窗。 c. 在新建云联网实例弹窗，输入所需参数单击**确定**，即可完成新建云联网实例。

> **说明：**
>
> 专线网关：请选择您和非腾讯云机房通信连接的专线网关。
>
> 私有网络：请选择步骤2中选择的 VPC 实例。
>
> 如出现 IP 地址段冲突，请返回步骤2重新选择或新建一个不会冲突的 VPC 实例。

1. 回到主机安全控制台，参考步骤1获取安装命令进行安装。您的非云平台机房需要放通对步骤1中描述的 IP 的5574、8080、80、9080共4个端口的访问。

热点问题

最近更新时间: 2024-08-23 15:08:00

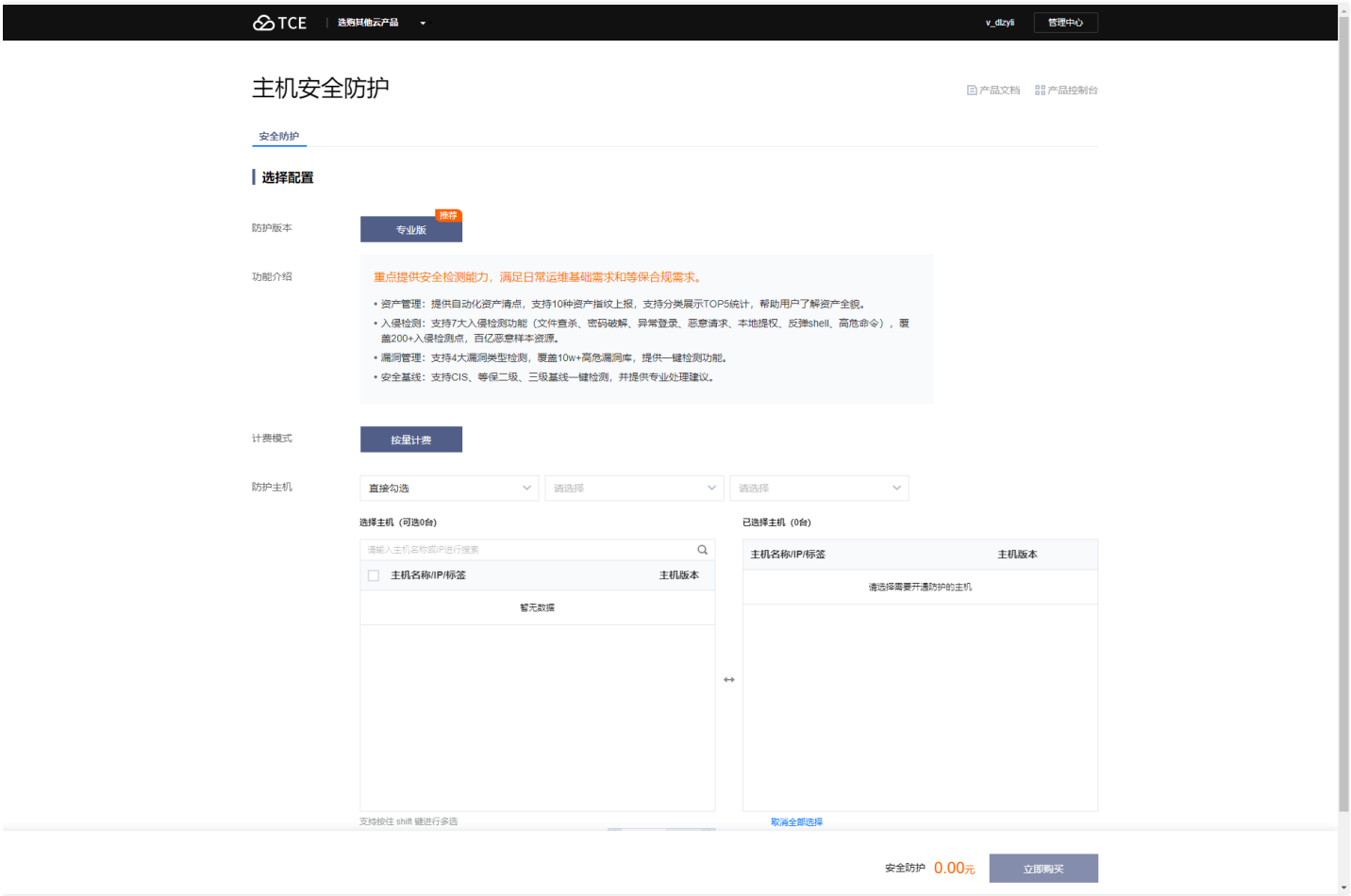
混合云是否对主机安全的版本有要求？

有的，必须是**专业版**才支持混合云的功能。

如何将主机安全升级至专业版？

1. 登录主机安全控制台，在左侧导航栏，选择**设置中心**>**授权管理**>**购买防护授权**，进入支付页面。

   在支付页面里，可输入要购买的授权数（专业版），根据需求选择后单击**立即购买**。



专线连接到云端，目标地址和开放端口是多少？

请参考下图的目标地址和开放端口，放通防火墙权限。

> **说明：**
>
> 地址和开放端口是不会变化。

防火墙拦截

建议防火墙策略放过主机安全后台服务器访问地址

基础网络域名	s.yd.qcloud.com、l.yd.qcloud.com、u.yd.qcloud.com	基础网络端口	5574、8080、80、9080
VPC网络域名	s.yd.tencentyun.com、l.yd.tencentyun.com、u.yd.tencentyun.com	VPC网络端口	5574、8080、80、9080
公网域名	sp.yd.qcloud.com、lp.yd.qcloud.com、up.yd.qcloud.com		
公网端口	5574、8080、80、443、9080		

国外的 IDC 是否支持安装 Agent?

支持的，目前只要机器能够联网，系统满足要求，就可以安装主机安全 Agent。

安装 Agent 后，控制台目前多久会展示非云平台机器？

目前是秒级支持。

非云平台机器，需要另外购买控制台吗？

不需要的，统一在公有云控制台进行管理、计费。

需要开 IDC 到云上的网络端口访问权限，目标 IP 和端口是什么？

目标 IP 是安装命令内的 IP，端口5574 80 8080 9080。

内网机器，无法访问公网或者没有专线的情况下是不是无法使用云镜？

目前是的。

混合云的客户端会和 Zabbix 进程冲突吗？

我们没有对 Zabbix 做特殊处理，也没有注入等，可以关注下机器上是否有其他的客户端安装驱动。

租户端操作介绍_旗舰版
Java内存马

最近更新时间: 2024-08-23 15:08:00

> **说明：**
>
> 本文档系旗舰版相关，如果您当前使用的不是旗舰版请忽略

Java内存马

概述

主机安全支持实时监控、捕捉 JavaWeb 服务进程内存中存在的未知 Class，结合尚航云_V1攻防经验及专家知识自动识别内存木马。若检测到 Java 内存马，系统会向您提供实时告警通知。

前提条件

Java 内存马属于主机安全专业版功能，须 升级专业版 才可使用该功能。

操作步骤

1. 登录 主机安全控制台，在左侧导航栏，选择**高级防御** > **Java 内存马**，进入 Java 内存马页面。

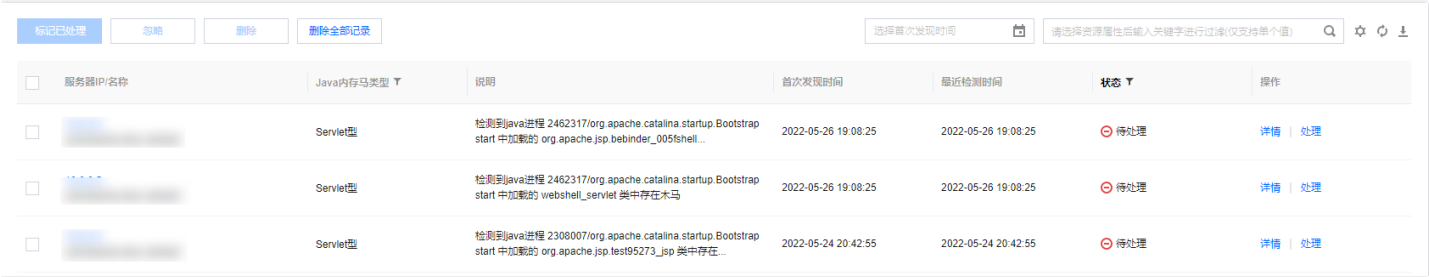
2. 选择**插件配置**，插件配置是监测 Java 内存马的前提，您可对专业版主机进行插件的开启和关闭，并观测插件的具体运行状态。

> **说明：**
>
> - 启用 Java 内存马插件后，主机安全会自动检测主机上 JavaWeb 服务进程，并注入检测探针到服务进程中，实时监控黑客通过漏洞、Shell 等注入的 Java 内存马。
> - 已成功注入 Java 内存马插件的主机，将实时监控、捕捉 JavaWeb 服务进程内存中存在的未知 Class，结合尚航云_V1攻防经验及专家知识自动识别内存木马。若检测到 Java 内存马，系统会向您提供实时告警通知。

字段说明：

- **启用/关闭插件**：Java 内存马插件默认关闭，支持用户手动设置开关，可单主机设置，也可多选主机批量设置。
- **插件状态**：全部正常、存在异常、未开启。
- **首次开启时间**：指首次启用插件的时间。
- **更新时间**：指近期启用或关闭插件的时间。
- **详情**：可查看当前已注入的 Java 内存马插件运行状态，包括进程 PID、进程主类名、插件状态（注入中、注入成功、插件超时、插入退出、注入失败）、错误日志。

启用 Java 内存马插件后，您可选择**事件列表**，可查看检测到的 Java 内存马事件，并进行相关处理操作。



字段说明：

- **Java 内存马类型**：包括 Filter 型、Listener 型、Servlet 型、Interceptors 型、Agent 型、其他。
- 说明：归纳说明 Java 内存马的概况。
- **首次发现时间**：该 Java 内存马首次被检测到的时间。
- **最近检测时间**：近期检测发现该 Java 内存马仍存在的时间。
- **状态**：待处理、已处理、已忽略。
- **操作**：
  - 单击**详情**可查看该内存马事件详情。

- 单击 Java 内存马详情中的**查看文件**，可查看落地文件的反编译 Java 文件，支持复制，支持下载反编译 Java 文件或原 Class 文件。

- 单击**处理**可对事件进行标记已处理、忽略、删除记录操作，可单事件处理，也可多选事件批量处理。

漏洞防御

最近更新时间: 2024-08-23 15:08:00

漏洞管理

漏洞防御

漏洞防御是尚航云_V1主机安全为应对频发的0DAY、nDAY 漏洞而开发的一套基于虚拟补丁的漏洞防御系统。该系统融合了腾讯前沿的漏洞挖掘技术、实时高危漏洞预警技术，捕捉、分析0DAY 漏洞，结合腾讯专家知识，生成虚拟补丁，自动在云服务器上生效虚拟补丁，有效拦截黑客攻击行为，为客户修复漏洞争取时间。

- 单击**一键防御**开关，您可选择防御主机范围并开启漏洞攻击拦截功能，实时拦截漏洞利用行为，避免业务被攻击利用。
- 漏洞防御开启后，单击**详情**可查看当前主机防御插件状态（正常/异常）、进程 PID、进程主类名、错误日志等。
- 单击**防御设置**也可对防御开关、防御主机范围进行设置，设置后可立即生效。
- 在**漏洞防御**区域内，可通过攻防曲线图，直观了解当前漏洞攻击频率和防御情况。

漏洞攻击事件列表

在**漏洞攻击事件**中，您可查看尝试攻击事件和防御成功事件，并支持对事件进行处理。

漏洞攻击事件类型	描述
尝试攻击事件	基于腾讯 WeDetect 云上威胁狩猎系统，自动化检测漏洞攻击行为。结合入侵事件中产生的漏洞、进程等多维度数据，实时对攻击事件进行自动化关联分析，及时响应并阻止利用已知/未知漏洞的攻击。
防御成功事件	在已开启漏洞防御功能状态下，已拦截成功的漏洞攻击行为。

漏洞攻击事件列表各字段说明：

- 被攻击漏洞名称/CVE 编号：存在该漏洞的主机发生了被攻击事件。
- 入侵状态：尝试攻击、防御成功。
- 攻击源 IP/地址：攻击来源的主机及其所在地址。
- 被攻击主机/IP：存在该漏洞的主机。

- 首次发生时间：首次检测到攻击事件的时间。
- 最近更新时间：最近检测到攻击事件的时间。
- 事件数量：攻击次数。
- 处理状态：待处理、已防御、已处理、已忽略。

操作

- 详情：单击**详情**可查看漏洞攻击事件详情，含危害描述、修复建议、网络攻击信息、服务进程信息等。

处理

- 修复漏洞：单击**修复漏洞**将打开漏洞详情，可按照修复建议进行修复。
- 标记已处理：此次标记仅针对本事件，若下次发生相同事件，仍会产生安全事件。
- 忽略：此次忽略仅针对本事件，若下次发生相同事件，仍会产生安全事件。
- 删除记录：删除该事件记录，控制台将不再显示，无法恢复记录，请慎重操作。

云镜软件相关说明
功能行为描述

最近更新时间: 2024-08-23 15:08:00

Webshell 检测

Webshell 是黑客入侵过程中常用工具，主机安全客户端会对服务器上新创建的 Web 程序文件进行可疑风险判断，对于少量疑似 Webshell 文件，需要上报到云端，通过云端的机器学习检测引擎模块做进一步检测，检测完成后会实时删除该样本文件。主机安全默认提供每天全盘扫描服务，检测过程不会提取任何涉及用户隐私的数据。

登录异常提醒

登录异常提醒功能可以帮助用户识别异常的管理员登录行为，需要采集登录日志中的来源 IP、时间、登录用户名、登录状态数据到云端进行风险计算，登录日志数据需在云端保存一个月。

密码破解提醒

密码破解提醒功能可以告诉用户当前遭受的密码破解事件和破解结果，需要采集登录日志中的来源 IP、时间、登录用户名、登录状态数据到云端进行风险计算，登录日志数据需在云端保存一个月。

恶意木马和病毒检测

恶意木马和病毒程序通常会窃取用户数据或者对外攻击，消耗大量系统资源导致业务不能正常提供服务。客户端会采集可疑恶意程序的哈希指纹到云端，通过云查杀模块对哈希指纹进行检测，若云端哈希库无该文件记录，需要上报可执行文件到云端，通过云端杀毒引擎进行检测，检测完后会实时删除该样本文件。主机安全默认提供每天全盘扫描服务，检测过程中不会提取任何涉及用户隐私的数据。

漏洞提醒

目前主机安全支持检测影响面较大的 Linux 和 Windows 双平台的漏洞，以及符合尚航云_V1安全要求的基线检测。 漏洞管理功能会显示当前主机上的漏洞风险情况，同时提供修复方案供用户参考。该模块执行时会从云端下载漏洞策略库在本地执行检测，对于存在漏洞风险的主机，会上报应用软件的名称、版本号、路径、发现时间。主机安全默认提供每天漏洞扫描服务，这个过程不会提取任何涉及用户隐私的数据。

升级维护

升级维护功能主要提醒用户对客户端进行升级，以获得最新的安全防护服务，客户端软件需要采集主机安全版本号、操作系统配置信息、安全规则版本号到云端进行判断和提醒，该过程不会提取任何涉及用户隐私的数据。

客户端进程说明

最近更新时间: 2024-08-23 15:08:00

名称	Windows 系统	Linux 系统
程序安装目录	C:\program files\qcloud\yunjing\ydeyes C:\program files\qcloud\yunjing\ydlive	/usr/local/qcloud/YunJing/
进程名称	YDService 云镜主服务进程 YDLive 守护进程 YDPython 漏洞&基线扫描插件 YDQuaraV2 木马隔离插件 qtflame 资产采集插件	YDService 云镜主服务进程 YDLive 守护进程 YDPython 漏洞&基线扫描插件 YDUtils 进程扫描插件 YDQuaraV2 木马隔离插件 qtflame 资产采集插件 tcss-agent 容器基线扫描插件 css-scan 容器镜像扫描插件
注册服务名称	YDService YDLive YDEdr	-

客户端程序所占用端口是系统随机返回的，无固定端口范围，若占用端口与用户业务端口冲突，重启客户端程序即可。

- 客户端重启命令（Linux系统）

1. 暂停客户端程序服务

```
/usr/local/qcloud/YunJing/stopYDCore.sh
```

2. 重新启动客户端

```
/usr/local/qcloud/YunJing/startYD.sh
```

- 客户端重启命令（Windows系统）输入以下命令，或打开任务管理器的服务，找到 YDService 服务，右键重启。

1. 暂停客户端程序服务

```
net stop YDService
```

2. 重新启动客户端

```
net start YDService
```

安全基线检测列表

最近更新时间: 2024-08-23 15:08:00

本文档将为您介绍主机安全的安全基线检测列表。

> 注意：
>
> 安全基线在产品设置后，将即时生效。

Name	Level	Vul_type
CouchDB 未授权访问	高	配置不当
Docker Daemon 2375 管理端口开启	高	远程代码执行
Elasticsearch 未授权访问	高	配置不当
JavaRMI 远程代码执行	高	远程代码执行
Jenkins 未开启认证可导致命令执行	高	远程代码执行
Kubelet 未授权访问	高	安全基线
Linux 系统弱口令检测	高	远程代码执行
MongoDB 未授权访问	高	配置不当
MySQL 弱口令检测	高	弱口令
NFS 错误配置导致可挂载敏感目录	高	配置不当
Redis 基线合规检测	高	远程代码执行
RPCBind 配置不当检测	高	安全基线
Rsync 弱口令检测	高	弱口令
Rsync 无密码访问	高	配置不当
Tomcat 弱口令检测	高	弱口令
Windows 用户弱口令检测	高	弱口令
Xampp 默认 FTP 密码	高	信息泄露
网站目录存在备份文件	高	信息泄露
FTP 匿名登录检测	中	信息泄露
IIS 配置错误导致存在解析漏洞	中	配置不当
Memcached UDP 端口可被利用为 DDOS 放大攻击	中	信息泄露
PHP-FPM 错误配置	中	安全基线
PostgreSQL 合规检测	中	远程代码执行
Web 目录存在 .git 文件夹导致信息泄露	中	信息泄露
Web 目录存在 .svn 文件夹导致信息泄露	中	信息泄露
Windows 隐藏账户检测	中	安全基线
Windows 影子账户检测	中	远程代码执行
ZooKeeper 未授权访问	中	配置不当
Hadoop未授权访问	低	远程代码执行
sudo 无密码用户检测	低	安全基线
Tomcat 样例目录检测	低	安全基线

Name	Level	Vul_type
Web 目录存在 phpinfo 文件	低	信息泄露
Windows 来宾账户状态检测	低	安全基线

API文档
主机安全（cwp）

版本（2018-02-28）
API概览

最近更新时间: 2024-09-03 18:50:01

API版本

V3

专家服务相关接口

接口名称	接口功能
DescribeAvailableExpertServiceDetail	可用订单详情
DescribeEmergencyResponseList	应急响应列表
DescribeExpertServiceList	安全管家列表
DescribeExpertServiceOrderList	专家服务订单列表
DescribeMonthInspectionReport	安全管家月巡检报告下载
DescribeProtectNetList	旗舰重保列表

入侵检测-反弹shell相关接口

接口名称	接口功能
DeleteReverseShellEvents	删除反弹Shell事件
DeleteReverseShellRules	删除反弹Shell规则
DescribeReverseShellEvents	获取反弹Shell列表
DescribeReverseShellRules	获取反弹Shell规则列表
ExportReverseShellEvents	导出反弹Shell事件

入侵检测-密码破解相关接口

接口名称	接口功能
DeleteBruteAttacks	删除暴力破解记录
DescribeBanMode	获取爆破阻断模式
DescribeBanRegions	获取阻断地域
DescribeBanStatus	获取阻断按钮状态
DescribeBanWhiteList	获取阻断白名单列表
DescribeBruteAttackList	获取密码破解列表
DescribeBruteAttackRules	获取爆破破解规则
ExportBruteAttacks	导出密码破解记录
ModifyBanMode	修改爆破阻断模式
ModifyBanStatus	设置阻断开关状态

接口名称	接口功能
ModifyBruteAttackRules	修改暴力破解规则
StopNoticeBanTips	不再提醒爆破阻断提示弹窗

入侵检测-异常登录相关接口

接口名称	接口功能
DeleteLoginWhiteList	删除异地登录白名单规则
DeleteNonlocalLoginPlaces	删除异地登录记录
DescribeHostLoginList	获取登录审计列表
DescribeLoginWhiteCombinedList	获取异地登录白名单合并后列表
DescribeLoginWhiteList	获取异地登录白名单列表
DescribeUsualLoginPlaces	查询常用登录地
ExportNonlocalLoginPlaces	导出异地登录记录

入侵检测-恶意请求相关接口

接口名称	接口功能
DeleteMaliciousRequests	删除恶意请求记录
DescribeMaliciousRequestWhiteList	查询恶意请求白名单列表
DescribeRiskDnsList	获取恶意请求列表
ExportMaliciousRequests	导出下载恶意请求文件

入侵检测-文件查杀相关接口

接口名称	接口功能
CreateNetAttackWhiteList	创建网络攻击白名单
CreateScanMalwareSetting	文件查杀检测
DeleteMalwareScanTask	入侵管理-终止扫描任务
DeleteMalwares	删除木马记录
DeleteNetAttackWhiteList	删除网络攻击白名单
DescribeJavaMemShellList	查询java内存马事件列表
DescribeMalWareList	获取木马列表
DescribeMalwareFile	获取木马文件下载地址
DescribeMalwareInfo	查看恶意文件详情
DescribeMalwareRiskWarning	风险预警提示
DescribeMalwareTimingScanSetting	查询定时扫描配置
DescribeNetAttackWhiteList	获取网络攻击白名单列表
DescribeScanMalwareSchedule	查询木马扫描进度

接口名称	接口功能
DescribeServersAndRiskAndFirstInfo	获文件查杀概览信息
ExportMalwares	导出木马记录
ModifyMalwareTimingScanSettings	定时扫描设置
ModifyNetAttackWhiteList	编辑网络攻击白名单
RecoverMalwares	恢复木马文件
SeparateMalwares	隔离木马
TrustMalwares	信任木马文件
UntrustMalwares	取消信任木马

入侵检测-本地提权相关接口

接口名称	接口功能
DeletePrivilegeEvents	删除本地提权事件
DeletePrivilegeRules	删除本地提权规则
DescribePrivilegeEvents	获取本地提权事件列表
DescribePrivilegeRules	获取本地提权规则列表
ExportPrivilegeEvents	导出本地提权事件

入侵检测-高危命令相关接口

接口名称	接口功能
CheckBashRuleParams	校验高危命新增用户规则参数
DeleteBashEvents	删除高危命令事件
DeleteBashRules	删除高危命令规则
DescribeBashEvents	获取高危命令列表
DescribeBashEventsNew	获取高危命令列表(新)
DescribeBashRules	获取高危命令规则列表
EditBashRules	新增或修改高危命令规则（支持多服务器选择）
ExportBashEvents	导出高危命令事件
SetBashEventsStatus	设置高危命令事件状态
SwitchBashRules	切换高危命令规则状态

其他接口

接口名称	接口功能
DeleteScanTask	停止扫描任务
DescribeAssetEnvList	查询资产管理环境变量列表
DescribeClientException	获取客户端异常事件

接口名称	接口功能
DescribeGeneralStat	获取主机相关统计
DescribeOverviewStatistics	获取概览统计数据
DescribeProVersionInfo	获取专业版概览信息
DescribeProVersionStatus	获取专业版状态
DescribeScanState	查询扫描状态
DescribeScanTaskDetails	查询扫描任务详情
DescribeScanTaskStatus	查询机器扫描状态列表
DescribeSecurityDynamics	获取安全事件动态消息
DescribeSecurityEventStat	获取安全事件统计
DescribeSecurityEventsCnt	获取安全事件数统计数据
DescribeSecurityTrends	获取安全事件统计数据
DescribeTaskDuration	获取任务下发时长
DescribeVersionStatistics	获取专业版和基础版机器数
ExportScanTaskDetails	导出扫描任务详情
ExportSecurityTrends	导出风险趋势
ExportTasks	异步导出任务
ModifyEventAttackStatus	修改网络攻击事件状态

基线管理相关接口

接口名称	接口功能
ChangeRuleEventsIgnoreStatus	修改事件忽略状态
CreateBaselineStrategy	创建基线策略
DeleteBaselineStrategy	删除基线策略
DescribeBaselineAnalysisData	基线策略概览统计数据查询
DescribeBaselineBasicInfo	查询基线基础信息
DescribeBaselineDetail	查询基线详情
DescribeBaselineEffectHostList	基线影响主机列表
DescribeBaselineHostTop	服务器风险top接口
DescribeBaselineList	查询基线列表
DescribeBaselineRule	查询基线检测项信息
DescribeBaselineScanSchedule	基线检测进度查询
DescribeBaselineStrategyDetail	查询基线策略详情
DescribeBaselineStrategyList	用户基线策略列表查询
DescribeBaselineTop	基线检测项TOP
DescribeIgnoreBaselineRule	查询忽略检测项信息
DescribeIgnoreRuleEffectHostList	查询忽略检测项影响主机列表

接口名称	接口功能
DescribeStrategyExist	根据策略名查询策略是否存在
ExportBaselineEffectHostList	基线影响主机列表导出
ExportBaselineList	导出基线列表
ExportIgnoreBaselineRule	已忽略基线检测项导出
ExportIgnoreRuleEffectHostList	忽略检测项影响主机列表导出
UpdateBaselineStrategy	更新基线策略信息

安全运营相关接口

接口名称	接口功能
CreateSearchLog	添加历史搜索记录
CreateSearchTemplate	添加检索模板
DeleteSearchTemplate	删除检索模板
DescribeESAggregations	获取ES字段聚合结果
DescribeHistoryService	查询日志检索服务信息
DescribeIndexList	获取索引列表
DescribeLogStorageStatistic	获取日志检索容量使用统计
DescribeSearchExportList	导出ES查询文档列表
DescribeSearchLogs	获取历史搜索记录
DescribeSearchTemplates	获取快速检索列表

新版基线管理相关接口

接口名称	接口功能
DeleteBaselinePolicy	删除基线策略配置
DeleteBaselineRule	删除基线规则
DeleteBaselineRuleIgnore	删除基线忽略规则
DeleteBaselineWeakPassword	删除基线弱口令
DescribeBaselineDetectList	获取基线检测详情记录
DescribeBaselineDetectOverview	获取基线检测概览
DescribeBaselineDownloadList	获取基线下载列表
DescribeBaselineFixList	获取基线修复列表
DescribeBaselineHostDetectList	获取基线检测主机列表
DescribeBaselineHostIgnoreList	获取忽略规则主机列表
DescribeBaselineHostRiskTop	获取基线服务器风险TOP5
DescribeBaselineItemDetectList	获取基线检测项的列表
DescribeBaselineItemIgnoreList	获取忽略规则项列表

接口名称	接口功能
DescribeBaselineItemInfo	获取基线检测项信息
DescribeBaselineItemList	获取基线项检测结果列表
DescribeBaselineItemRiskTop	获取基线检测项TOP5
DescribeBaselinePolicyList	获取基线策略列表
DescribeBaselineRuleCategoryList	获取基线分类列表
DescribeBaselineRuleDetectList	获取基线规则检测列表
DescribeBaselineRuleIgnoreList	获取基线忽略规则列表
DescribeBaselineRuleList	获取基线规则列表
DescribeBaselineWeakPasswordList	获取基线弱口令列表
DescribeHotVulTop	获取全网热点漏洞
DescribeIgnoreHostAndItemConfig	获取一键忽略受影响的检测项和主机信息
DescribeVulStoreList	获取漏洞库列表
ExportBaselineFixList	导出修复列表
ExportBaselineHostDetectList	导出基线主机检测
ExportBaselineItemDetectList	导出基线检测项
ExportBaselineItemList	导出检测项结果列表
ExportBaselineRuleDetectList	导出基线检测规则
ExportBaselineWeakPasswordList	导出弱口令配置列表
FixBaselineDetect	修复基线检测
ModifyBaselinePolicy	修改或新增基线策略设置
ModifyBaselinePolicyState	修改或新增基线策略状态
ModifyBaselineRule	修改或新增基线检测规则
ModifyBaselineRuleIgnore	修改或新增基线忽略规则
ModifyBaselineWeakPassword	修改或新增弱口令
StartBaselineDetect	检测基线
StopBaselineDetect	停止基线检测
SyncBaselineDetectSummary	同步基线检测进度概要

漏洞管理相关接口

接口名称	接口功能
CancelIgnoreVul	取消漏洞忽略
CreateEmergencyVulScan	应急漏洞扫描
DescribeEmergencyVulList	应急漏洞列表
DescribeScanSchedule	查询检测进度
DescribeScanVulSetting	定期检测配置查询
DescribeUndoVulCounts	获取指定漏洞分类统计数

接口名称	接口功能
DescribeVulCountByDates	获取近日指定类型的漏洞数量和主机数量
DescribeVulEffectHostList	漏洞影响主机列表
DescribeVulHostCountScanTime	获取待处理漏洞数+影响主机数
DescribeVulHostTop	获取服务器风险top列表
DescribeVulInfoCvss	漏洞详情
DescribeVulLevelCount	查询漏洞数量等级分布统计
DescribeVulList	漏洞列表
DescribeVulTop	获取漏洞top统计
ExportVulDetectionExcel	导出本次漏洞检测Excel
ExportVulDetectionReport	导出漏洞检测报告
ExportVulEffectHostList	导出漏洞影响主机列表
ExportVulList	漏洞管理-导出漏洞列表
IgnoreImpactedHosts	忽略漏洞
ScanVul	一键检测
ScanVulAgain	漏洞管理-重新检测接口
ScanVulSetting	定期扫描漏洞设置

设置中心相关接口

接口名称	接口功能
CreateLicenseOrder	创建授权订单
DeleteLicenseRecord	删除授权记录
DescribeLicenseBindList	查看授权绑定列表
DescribeLicenseBindSchedule	查询授权绑定进度
DescribeLicenseGeneral	授权概览信息
DescribeLicenseList	获取授权订单列表
DescribeSaveOrUpdateWarnings	更新用户告警设置
DescribeWarningList	获取当前用户告警列表
DestroyOrder	销毁订单
ExportLicenseDetail	导出授权详情
ModifyAutoOpenProVersionConfig	设置自动开通配置
ModifyLicenseBinds	授权批量绑定
ModifyLicenseUnBinds	授权批量解绑
ModifyOrderAttribute	编辑订单属性
ModifyWarningSetting	修改告警设置

资产管理相关接口

接口名称	接口功能
DeleteMachine	卸载云镜客户端
DeleteMachineTag	删除服务器关联的标签
DeleteTags	删除标签
DescribeAccountStatistics	获取帐号统计列表数据
DescribeAssetAppList	查询应用列表
DescribeAssetAppProcessList	获取软件关联进程列表
DescribeAssetCoreModuleInfo	获取内核模块详情
DescribeAssetCoreModuleList	查询资产管理内核模块列表
DescribeAssetDatabaseInfo	获取资产管理数据库详情
DescribeAssetDatabaseList	查询资产管理数据库列表
DescribeAssetHostTotalCount	获取主机所有资源数量
DescribeAssetInfo	获取资产数量概况
DescribeAssetInitServiceList	查询资产管理启动服务列表
DescribeAssetJarInfo	获取Jar包详情
DescribeAssetJarList	查询Jar包列表
DescribeAssetMachineDetail	获取资产管理主机资源详细信息
DescribeAssetMachineList	获取资源监控列表
DescribeAssetPlanTaskList	查询资产管理计划任务列表
DescribeAssetPortInfoList	获取资产管理端口列表
DescribeAssetProcessInfoList	获取资产管理进程列表
DescribeAssetRecentMachineInfo	获取主机概况趋势
DescribeAssetSystemPackageList	获取资产管理系统安装包列表
DescribeAssetUserInfo	获取主机账号详情
DescribeAssetUserList	获取账号列表
DescribeAssetWebAppList	获取资产管理Web应用列表
DescribeAssetWebAppPluginList	获取资产管理Web应用插件列表
DescribeAssetWebFrameList	获取资产管理Web框架列表
DescribeAssetWebLocationInfo	获取Web站点详情
DescribeAssetWebLocationList	获取Web站点列表
DescribeAssetWebServiceInfoList	查询资产管理Web服务列表
DescribeAssetWebServiceProcessList	获取Web服务关联进程列表
DescribeComponentStatistics	获取组件统计列表
DescribeExportMachines	导出区域主机列表
DescribeHistoryAccounts	获取帐号变更历史列表
DescribeImportMachineInfo	查询批量导入机器信息
DescribeMachineInfo	获取机器详情

接口名称	接口功能
DescribeMachineOsList	查询机器操作系统列表
DescribeMachineRegions	获取机器地域列表
DescribeMachines	获取区域主机列表
DescribeOpenPortStatistics	获取端口统计列表
DescribeProcessStatistics	获取进程统计列表
DescribeTagMachines	获取指定标签关联的服务器信息
DescribeTags	获取所有主机标签
EditTags	新增或编辑标签
ExportAssetCoreModuleList	导出资产管理内核模块列表
ExportAssetWebServiceInfoList	导出资产管理Web服务列表
ModifyMachineRemark	修改主机备注信息
ScanAsset	资产指纹启动扫描
SyncAssetScan	同步资产扫描信息
UpdateMachineTags	关联机器标签列表

高级防御相关接口

接口名称	接口功能
CreateProtectServer	添加网站防护服务器
DeleteAttackLogs	删除网络攻击日志
DeleteProtectDir	删除防护网站
DeleteWebPageEventLog	删除事件记录
DescribeAttackEventInfo	网络攻击事件详情
DescribeAttackEvents	按分页形式展示网络攻击检测事件列表
DescribeAttackLogInfo	网络攻击日志详情
DescribeAttackLogs	网络攻击日志列表
DescribeAttackStatistics	网络攻击数据统计
DescribeAttackTop	网络攻击top5数据列表
DescribeAttackTrends	网络攻击趋势数据
DescribeAttackVulTypeList	获取网络攻击威胁类型列表
DescribeMachineList	网页防篡改获取区域主机列表
DescribeNetAttackSetting	查询网络攻击设置
DescribeProtectDirList	防护目录列表
DescribeProtectDirRelatedServer	查询防护目录关联服务器
DescribeServerRelatedDirInfo	查询服务器关联目录详情
DescribeWebPageEventList	查询篡改事件列表
DescribeWebPageGeneralize	查询网页防篡改概览信息

接口名称	接口功能
DescribeWebPageProtectStat	查询网页防篡改防护统计
DescribeWebPageServiceInfo	查询网站防篡改服务信息
ExportAttackEvents	导出网络攻击事件
ExportAttackLogs	导出网络攻击日志
ExportProtectDirList	导出防护目录列表
ExportWebPageEventList	导出篡改事件列表
ModifyNetAttackSetting	修改网络攻击设置
ModifyWebPageProtectDir	创建网站防护目录
ModifyWebPageProtectSetting	修改网站防护设置
ModifyWebPageProtectSwitch	网站防护设置开关

调用方式
接口签名v1

最近更新时间: 2024-09-03 18:50:01

tcecloud API 会对每个访问请求进行身份验证，即每个请求都需要在公共请求参数中包含签名信息（Signature）以验证请求者身份。 签名信息由安全凭证生成，安全凭证包括 SecretId 和 SecretKey；若用户还没有安全凭证，请前往云API密钥页面申请，否则无法调用云API接口。

1. 申请安全凭证

在第一次使用云API之前，请前往云API密钥页面申请安全凭证。 安全凭证包括 SecretId 和 SecretKey：

- SecretId 用于标识 API 调用者身份
- SecretKey 用于加密签名字符串和服务器端验证签名字符串的密钥。
- 用户必须严格保管安全凭证，避免泄露。

申请安全凭证的具体步骤如下：

1. 登录tcecloud管理中心控制台。
2. 前往云API密钥的控制台页面
3. 在云API密钥页面，点击【新建】即可以创建一对SecretId/SecretKey

注意：开发商帐号最多可以拥有两对 SecretId / SecretKey。

2. 生成签名串

有了安全凭证SecretId 和 SecretKey后，就可以生成签名串了。以下是生成签名串的详细过程：

假设用户的 SecretId 和 SecretKey 分别是：

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

注意：这里只是示例，请根据用户实际申请的 SecretId 和 SecretKey 进行后续操作！

以云服务器查看实例列表(DescribeInstances)请求为例，当用户调用这一接口时，其请求参数可能如下:

参数名称	中文	参数值
Action	方法名	DescribeInstances
SecretId	密钥Id	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	当前时间戳	1465185768
Nonce	随机正整数	11886
Region	实例所在区域	ap-guangzhou
InstanceIds.0	待查询的实例ID	ins-09dx96dg
Offset	偏移量	0
Limit	最大允许输出	20
Version	接口版本号	2017-03-12

2.1. 对参数排序

首先对所有请求参数按参数名的字典序（ ASCII 码）升序排序。注意：1）只按参数名进行排序，参数值保持对应即可，不参与比大小；2）按 ASCII 码比大小，如 InstanceIds.2 要排在 InstanceIds.12 后面，不是按字母表，也不是按数值。用户可以借助编程语言中的相关排序函数来实现这一功能，如 php 中的 ksort 函数。上述示例参数的排序结果如下:

```
{
'Action' : 'DescribeInstances',
'InstanceIds.0' : 'ins-09dx96dg',
'Limit' : 20,
'Nonce' : 11886,
'Offset' : 0,
'Region' : 'ap-guangzhou',
'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
'Timestamp' : 1465185768,
'Version': '2017-03-12',
}
```

使用其它程序设计语言开发时，可对上面示例中的参数进行排序，得到的结果一致即可。

2.2. 拼接请求字符串

此步骤生成请求字符串。 将把上一步排序好的请求参数格式化成“参数名称”=“参数值”的形式，如对 Action 参数，其参数名称为 "Action" ，参数值为 "DescribeInstances" ，因此格式化后就为 Action=DescribeInstances 。 **注意：“参数值”为原始值而非url编码后的值。**

然后将格式化后的各个参数用"&"拼接在一起，最终生成的请求字符串为:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.3. 拼接签名原文字符串

此步骤生成签名原文字符串。 签名原文字符串由以下几个参数构成:

1. 请求方法: 支持 POST 和 GET 方式，这里使用 GET 请求，注意方法为全大写。
2. 请求主机:查看实例列表(DescribeInstances)的请求域名为：cvm.cloud.sunhongs.com。实际的请求域名根据接口所属模块的不同而不同，详见各接口说明。
3. 请求路径: 当前版本云API的请求路径固定为 / 。
4. 请求字符串: 即上一步生成的请求字符串。

签名原文串的拼接规则为: 请求方法 + 请求主机 +请求路径 + ? + 请求字符串

示例的拼接结果为：

```
GETcvm.cloud.sunhongs.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.4. 生成签名串

此步骤生成签名串。 首先使用 HMAC-SHA1 算法对上一步中获得的**签名原文字符串**进行签名，然后将生成的签名串使用 Base64 进行编码，即可获得最终的签名串。

具体代码如下，以 PHP 语言为例:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.cloud.sunhongs.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

最终得到的签名串为:

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

使用其它程序设计语言开发时，可用上面示例中的原文进行签名验证，得到的签名串与例子中的一致即可。

3. 签名串编码

生成的签名串并不能直接作为请求参数，需要对其进行 URL 编码。

如上一步生成的签名串为 EliP9YW3pW28FpsEdkXt/+WcGeI= ，最终得到的签名串请求参数（Signature）为：EliP9YW3pW28FpsEdkXt%2f%2bWcGeI%3d，它将用于生成最终的请求 URL。

注意：如果用户的请求方法是 GET，或者请求方法为 POST 同时 Content-Type 为 application/x-www-form-urlencoded，则发送请求时所有请求参数的值均需要做 URL 编码，参数键和=符号不需要编码。非 ASCII 字符在 URL 编码前需要先以 UTF-8 进行编码。

注意：有些编程语言的 http 库会自动为所有参数进行 urlencode，在这种情况下，就不需要对签名串进行 URL 编码了，否则两次 URL 编码会导致签名失败。

注意：其他参数值也需要进行编码，编码采用 RFC 3986。使用 %XY 对特殊字符例如汉字进行百分比编码，其中"X"和"Y"为十六进制字符（0-9 和大写字母 A-F），使用小写将引发错误。

4. 签名失败

根据实际情况，存在以下签名失败的错误码，请根据实际情况处理

错误代码	错误描述
AuthFailure.SignatureExpire	签名过期
AuthFailure.SecretIdNotFound	密钥不存在
AuthFailure.SignatureFailure	签名错误
AuthFailure.TokenFailure	token 错误
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）

5. 签名演示

在实际调用 API 3.0 时，推荐使用配套的tcecloud SDK 3.0 ，SDK 封装了签名的过程，开发时只关注产品提供的具体接口即可。详细信息参见 SDK 中心。当前支持的编程语言有：

- Python
- Java
- PHP
- Go
- JavaScript
- .NET

为了更清楚的解释签名过程，下面以实际编程语言为例，将上述的签名过程具体实现。请求的域名、调用的接口和参数的取值都以上述签名过程为准，代码只为解释签名过程，并不具备通用性，实际开发请尽量使用 SDK 。

最终输出的 url 可能为： `https://cvm.cloud.sunhongs.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGeI%3D&Timestamp=1465185768&Version=2017-03-12`

注意：由于示例中的密钥是虚构的，时间戳也不是系统当前时间，因此如果将此 url 在浏览器中打开或者用 curl 等命令调用时会返回鉴权错误：签名过期。为了得到一个可以正常返回的 url ，需要修改示例中的 SecretId 和 SecretKey 为真实的密钥，并使用系统当前时间戳作为 Timestamp 。

注意：在下面的示例中，不同编程语言，甚至同一语言每次执行得到的 url 可能都有所不同，表现为参数的顺序不同，但这并不影响正确性。只要所有参数都在，且签名计算正确即可。

注意：以下代码仅适用于 API 3.0，不能直接用于其他的签名流程，即使是旧版的 API ，由于存在细节差异也会导致签名计算错误，请以对应的实际文档为准。

Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.util.Random;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class TceCloudAPIDemo {
private final static String CHARSET = "UTF-8";
```

```
public static String sign(String s, String key, String method) throws Exception {
Mac mac = Mac.getInstance(method);
SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
mac.init(secretKeySpec);
byte[] hash = mac.doFinal(s.getBytes(CHARSET));
return DatatypeConverter.printBase64Binary(hash);
}

public static String getStringToSign(TreeMap<String, Object> params) {
StringBuilder s2s = new StringBuilder("GETcvm.cloud.sunhongs.com/?");
// 签名时要求对参数进行字典排序，此处用TreeMap保证顺序
for (String k : params.keySet()) {
s2s.append(k).append("=").append(params.get(k).toString()).append("&");
}
return s2s.toString().substring(0, s2s.length() - 1);
}

public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException {
StringBuilder url = new StringBuilder("https://cvm.cloud.sunhongs.com/?");
// 实际请求的url中对参数顺序没有要求
for (String k : params.keySet()) {
// 需要对请求串进行urlencode，由于key都是英文字母，故此处仅对其value进行urlencode
url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).append("&");
}
return url.toString().substring(0, url.length() - 1);
}

public static void main(String[] args) throws Exception {
TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap可以自动排序
// 实际调用时应当使用随机数，例如：params.put("Nonce", new Random().nextInt(java.lang.Integer.MAX_VALUE));
params.put("Nonce", 11886); // 公共参数
// 实际调用时应当使用系统当前时间，例如： params.put("Timestamp", System.currentTimeMillis() / 1000);
params.put("Timestamp", 1465185768); // 公共参数
params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // 公共参数
params.put("Action", "DescribeInstances"); // 公共参数
params.put("Version", "2017-03-12"); // 公共参数
params.put("Region", "ap-guangzhou"); // 公共参数
params.put("Limit", 20); // 业务参数
params.put("Offset", 0); // 业务参数
params.put("InstanceIds.0", "ins-09dx96dg"); // 业务参数
params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE", "HmacSHA1")); // 公共参数
System.out.println(getUrl(params));
}
}
```

Python

注意：如果是在 Python 2 环境中运行，需要先安装 requests 依赖包： `pip install requests` 。

```
# -*- coding: utf8 -*-
import base64
import hashlib
import hmac
import time

import requests

secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

def get_string_to_sign(method, endpoint, params):
s = method + endpoint + "/?"
query_str = "&".join("%s=%s" % (k, params[k]) for k in sorted(params))
return s + query_str

def sign_str(key, s, method):
hmac_str = hmac.new(key.encode("utf8"), s.encode("utf8"), method).digest()
return base64.b64encode(hmac_str)

if __name__ == '__main__':
endpoint = "cvm.cloud.sunhongs.com"
```

```
data = {
'Action' : 'DescribeInstances',
'InstanceIds.0' : 'ins-09dx96dg',
'Limit' : 20,
'Nonce' : 11886,
'Offset' : 0,
'Region' : 'ap-guangzhou',
'SecretId' : secret_id,
'Timestamp' : 1465185768, # int(time.time())
'Version': '2017-03-12'
}
s = get_string_to_sign("GET", endpoint, data)
data["Signature"] = sign_str(secret_key, s, hashlib.sha1)
print(data["Signature"])
# 此处会实际调用，成功后可能产生计费
# resp = requests.get("https://" + endpoint, params=data)
# print(resp.url)
```

接口签名v3

最近更新时间: 2024-09-03 18:50:01

tcecloud API 会对每个访问请求进行身份验证，即每个请求都需要在公共请求参数中包含签名信息（Signature）以验证请求者身份。 签名信息由安全凭证生成，安全凭证包括 SecretId 和 SecretKey；若用户还没有安全凭证，请前往云API密钥页面申请，否则无法调用云API接口。

1. 申请安全凭证

在第一次使用云API之前，请前往云API密钥页面申请安全凭证。 安全凭证包括 SecretId 和 SecretKey：

- SecretId 用于标识 API 调用者身份
- SecretKey 用于加密签名字符串和服务器端验证签名字符串的密钥。
- 用户必须严格保管安全凭证，避免泄露。

申请安全凭证的具体步骤如下：

1. 登录tcecloud管理中心控制台。
2. 前往云API密钥的控制台页面
3. 在云API密钥页面，点击【新建】即可以创建一对SecretId/SecretKey

注意：开发商帐号最多可以拥有两对 SecretId / SecretKey。

2. TC3-HMAC-SHA256 签名方法

注意：对于GET方法，只支持 Content-Type: application/x-www-form-urlencoded 协议格式。对于POST方法，目前支持 Content-Type: application/json 以及 Content-Type: multipart/form-data 两种协议格式，json 格式默认所有业务接口均支持，multipart 格式只有特定业务接口支持，此时该接口不能使用 json 格式调用，参考具体业务接口文档说明。

下面以云服务器查询广州区实例列表作为例子，分步骤介绍签名的计算过程。我们仅用到了查询实例列表的两个参数：Limit 和 Offset，使用 GET 方法调用。

假设用户的 SecretId 和 SecretKey 分别是：AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE 和 Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

2.1. 拼接规范请求串

按如下格式拼接规范请求串（CanonicalRequest）：

```
CanonicalRequest =
HTTPRequestMethod + '\n' +
CanonicalURI + '\n' +
CanonicalQueryString + '\n' +
CanonicalHeaders + '\n' +
SignedHeaders + '\n' +
HashedRequestPayload
```

- HTTPRequestMethod：HTTP 请求方法（GET、POST ），本示例中为 GET；
- CanonicalURI：URI 参数，API 3.0 固定为正斜杠（/）；
- CanonicalQueryString：发起 HTTP 请求 URL 中的查询字符串，对于 POST 请求，固定为空字符串，对于 GET 请求，则为 URL 中问号（?）后面的字符串内容，本示例取值为：Limit=10&Offset=0。注意：CanonicalQueryString 需要经过 URL 编码。
- CanonicalHeaders：参与签名的头部信息，至少包含 host 和 content-type 两个头部，也可加入自定义的头部参与签名以提高自身请求的唯一性和安全性。拼接规则：1）头部 key 和 value 统一转成小写，并去掉首尾空格，按照 key:value\n 格式拼接；2）多个头部，按照头部 key（小写）的字典排序进行拼接。此例中为：content-type:application/x-www-form-urlencoded\nhost:cvm.cloud.sunhongs.com\n
- SignedHeaders：参与签名的头部信息，说明此次请求有哪些头部参与了签名，和 CanonicalHeaders 包含的头部内容是一一对应的。content-type 和 host 为必选头部。拼接规则：1）头部 key 统一转成小写；2）多个头部 key（小写）按照字典排序进行拼接，并且以分号（;）分隔。此例中为： content-type;host
- HashedRequestPayload：请求正文的哈希值，计算方法为 Lowercase(HexEncode(Hash.SHA256(RequestPayload)))，对 HTTP 请求整个正文 payload 做 SHA256 哈希，然后十六进制编码，最后编码串转换成小写字母。注意：对于 GET 请求，RequestPayload 固定为空字符串，对于 POST 请求，RequestPayload 即为 HTTP 请求正文 payload。

根据以上规则，示例中得到的规范请求串如下（为了展示清晰，\n 换行符通过另起打印新的一行替代）：

```
GET
/
Limit=10&Offset=0
content-type:application/x-www-form-urlencoded
host:cvm.cloud.sunhongs.com

content-type;host
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

2.2. 拼接待签名字符串

按如下格式拼接待签名字符串：

```
StringToSign =
Algorithm + \n +
RequestTimestamp + \n +
CredentialScope + \n +
HashedCanonicalRequest
```

- Algorithm：签名算法，目前固定为 TC3-HMAC-SHA256；
- RequestTimestamp：请求时间戳，即请求头部的 X-TC-Timestamp 取值，如上示例请求为 1539084154；
- CredentialScope：凭证范围，格式为 Date/service/tc3_request，包含日期、所请求的服务和终止字符串（tc3_request）。**Date 为 UTC 标准时间的日期，取值需要和公共参数 X-TC-Timestamp 换算的 UTC 标准时间日期一致**；service 为产品名，必须与调用的产品域名一致，例如 cvm。如上示例请求，取值为 2018-10-09/cvm/tc3_request；
- HashedCanonicalRequest：前述步骤拼接所得规范请求串的哈希值，计算方法为 Lowercase(HexEncode(Hash.SHA256(CanonicalRequest)))。

注意：

1. Date 必须从时间戳 X-TC-Timestamp 计算得到，且时区为 UTC+0。如果加入系统本地时区信息，例如东八区，将导致白天和晚上调用成功，但是凌晨时调用必定失败。假设时间戳为 1551113065，在东八区的时间是 2019-02-26 00:44:25，但是计算得到的 Date 取 UTC+0 的日期应为 2019-02-25，而不是 2019-02-26。
2. Timestamp 必须是当前系统时间，且需确保系统时间和标准时间是同步的，如果相差超过五分钟则必定失败。如果长时间不和标准时间同步，可能导致运行一段时间后，请求必定失败（返回签名过期错误）。

根据以上规则，示例中得到的待签名字符串如下（为了展示清晰，\n 换行符通过另起打印新的一行替代）：

```
TC3-HMAC-SHA256
1539084154
2018-10-09/cvm/tc3_request
91c9c192c14460df6c1ffc69e34e6c5e90708de2a6d282cccf957dbf1aa7f3a7
```

2.3. 计算签名

1）计算派生签名密钥，伪代码如下

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

- SecretKey：原始的 SecretKey；
- Date：即 Credential 中的 Date 字段信息，如上示例，为2018-10-09；
- Service：即 Credential 中的 Service 字段信息，如上示例，为 cvm；

2）计算签名，伪代码如下

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

- SecretSigning：即以上计算得到的派生签名密钥；
- StringToSign：即步骤2计算得到的待签名字符串；

2.4. 拼接 Authorization

按如下格式拼接 Authorization：

```
Authorization =
Algorithm + ' ' +
'Credential=' + SecretId + '/' + CredentialScope + ', ' +
'SignedHeaders=' + SignedHeaders + ', '
'Signature=' + Signature
```

- Algorithm：签名方法，固定为 TC3-HMAC-SHA256；
- SecretId：密钥对中的 SecretId；
- CredentialScope：见上文，凭证范围；
- SignedHeaders：见上文，参与签名的头部信息；
- Signature：签名值

根据以上规则，示例中得到的值为：

```
TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

最终完整的调用信息如下：

```
https://cvm.cloud.sunhongs.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.cloud.sunhongs.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: ap-guangzhou
```

3. 签名失败

根据实际情况，存在以下签名失败的错误码，请根据实际情况处理

错误代码	错误描述
AuthFailure.SignatureExpire	签名过期
AuthFailure.SecretIdNotFound	密钥不存在
AuthFailure.SignatureFailure	签名错误
AuthFailure.TokenFailure	token 错误
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）

4. 签名演示

Java

```
import java.io.BufferedReader;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.net.URL;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Map;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.net.ssl.HttpsURLConnection;
import javax.xml.bind.DatatypeConverter;
```

```
import org.apache.commons.codec.digest.DigestUtils;

public class TceCloudAPITC3Demo {
private final static String CHARSET = "UTF-8";
private final static String ENDPOINT = "cvm.cloud.sunhongs.com";
private final static String PATH = "/";
private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE";
private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE";
private final static String CT_X_WWW_FORM_URLENCODED = "application/x-www-form-urlencoded";
private final static String CT_JSON = "application/json";
private final static String CT_FORM_DATA = "multipart/form-data";

public static byte[] sign256(byte[] key, String msg) throws Exception {
Mac mac = Mac.getInstance("HmacSHA256");
SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
mac.init(secretKeySpec);
return mac.doFinal(msg.getBytes(CHARSET));
}

public static void main(String[] args) throws Exception {
String service = "cvm";
String host = "cvm.cloud.sunhongs.com";
String region = "ap-guangzhou";
String action = "DescribeInstances";
String version = "2017-03-12";
String algorithm = "TC3-HMAC-SHA256";
String timestamp = "1539084154";
//String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
// 注意时区，否则容易出错
sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

// ************ 步骤 1：拼接规范请求串 ************
String httpRequestMethod = "GET";
String canonicalUri = "/";
String canonicalQueryString = "Limit=10&Offset=0";
String canonicalHeaders = "content-type:application/x-www-form-urlencoded\n" + "host:" + host + "\n";
String signedHeaders = "content-type;host";
String hashedRequestPayload = DigestUtils.sha256Hex("");
String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryString + "\n"
+ canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
System.out.println(canonicalRequest);

// ************ 步骤 2：拼接待签名字符串 ************
String credentialScope = date + "/" + service + "/" + "tc3_request";
String hashedCanonicalRequest = DigestUtils.sha256Hex(canonicalRequest.getBytes(CHARSET));
String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCanonicalRequest;
System.out.println(stringToSign);

// ************ 步骤 3：计算签名 ************
byte[] secretDate = sign256(("TC3" + SECRET_KEY).getBytes(CHARSET), date);
byte[] secretService = sign256(secretDate, service);
byte[] secretSigning = sign256(secretService, "tc3_request");
String signature = DatatypeConverter.printHexBinary(sign256(secretSigning, stringToSign)).toLowerCase();
System.out.println(signature);

// ************ 步骤 4：拼接 Authorization ************
String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
+ "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
System.out.println(authorization);

TreeMap<String, String> headers = new TreeMap<String, String>();
headers.put("Authorization", authorization);
headers.put("Host", host);
headers.put("Content-Type", CT_X_WWW_FORM_URLENCODED);
headers.put("X-TC-Action", action);
headers.put("X-TC-Timestamp", timestamp);
headers.put("X-TC-Version", version);
headers.put("X-TC-Region", region);
}
}
```

Python

```
# -*- coding: utf-8 -*-
import hashlib, hmac, json, os, sys, time
from datetime import datetime

# 密钥参数
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.cloud.sunhongs.com"
endpoint = "https://" + host
region = "ap-guangzhou"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
timestamp = 1539084154
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 10, "Offset": 0}

# ********** 步骤 1：拼接规范请求串 **********
http_request_method = "GET"
canonical_uri = "/"
canonical_querystring = "Limit=10&Offset=0"
ct = "x-www-form-urlencoded"
payload = ""
if http_request_method == "POST":
canonical_querystring = ""
ct = "json"
payload = json.dumps(params)
canonical_headers = "content-type:application/%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
hashed_request_payload = hashlib.sha256(payload.encode("utf-8")).hexdigest()
canonical_request = (http_request_method + "\n" +
canonical_uri + "\n" +
canonical_querystring + "\n" +
canonical_headers + "\n" +
signed_headers + "\n" +
hashed_request_payload)
print(canonical_request)

# ********** 步骤 2：拼接待签名字符串 **********
credential_scope = date + "/" + service + "/" + "tc3_request"
hashed_canonical_request = hashlib.sha256(canonical_request.encode("utf-8")).hexdigest()
string_to_sign = (algorithm + "\n" +
str(timestamp) + "\n" +
credential_scope + "\n" +
hashed_canonical_request)
print(string_to_sign)


# ********** 步骤 3：计算签名 **********
# 计算签名摘要函数
def sign(key, msg):
return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()
secret_date = sign(("TC3" + secret_key).encode("utf-8"), date)
secret_service = sign(secret_date, service)
secret_signing = sign(secret_service, "tc3_request")
signature = hmac.new(secret_signing, string_to_sign.encode("utf-8"), hashlib.sha256).hexdigest()
print(signature)

# ********** 步骤 4：拼接 Authorization **********
authorization = (algorithm + " " +
"Credential=" + secret_id + "/" + credential_scope + ", " +
"SignedHeaders=" + signed_headers + ", " +
"Signature=" + signature)
print(authorization)

# 公共参数添加到请求头部
```

```
headers = {
"Authorization": authorization,
"Host": host,
"Content-Type": "application/%s" % ct,
"X-TC-Action": action,
"X-TC-Timestamp": str(timestamp),
"X-TC-Version": version,
"X-TC-Region": region,
}
```

请求结构

最近更新时间: 2024-09-03 18:50:01

1. 服务地址

地域（Region）是指物理的数据中心的地理区域。tcecloud交付验证不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议您选择最靠近您客户的地域。

您可以通过 API接口 **查询地域列表** 查看完成的地域列表。

2. 通信协议

tcecloud API 的所有接口均通过 HTTPS 进行通信，提供高安全性的通信通道。

3. 请求方法

支持的 HTTP 请求方法:

- POST（推荐）
- GET

POST 请求支持的 Content-Type 类型：

- application/json（推荐），必须使用 TC3-HMAC-SHA256 签名方法。
- application/x-www-form-urlencoded，必须使用 HmacSHA1 或 HmacSHA256 签名方法。
- multipart/form-data（仅部分接口支持），必须使用 TC3-HMAC-SHA256 签名方法。

GET 请求的请求包大小不得超过 32 KB。POST 请求使用签名方法为 HmacSHA1、HmacSHA256 时不得超过 1 MB。POST 请求使用签名方法为 TC3-HMAC-SHA256 时支持 10 MB。

4. 字符编码

均使用UTF-8编码。

返回结果

最近更新时间: 2024-09-03 18:50:01

正确返回结果

以云服务器的接口查看实例状态列表 (DescribeInstancesStatus) 2017-03-12 版本为例，若调用成功，其可能的返回如下为：

```
{
"Response": {
"TotalCount": 0,
"InstanceStatusSet": [],
"RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
}
}
```

- Response 及其内部的 RequestId 是固定的字段，无论请求成功与否，只要 API 处理了，则必定会返回。
- RequestId 用于一个 API 请求的唯一标识，如果 API 出现异常，可以联系我们，并提供该 ID 来解决问题。
- 除了固定的字段外，其余均为具体接口定义的字段，不同的接口所返回的字段参见接口文档中的定义。此例中的 TotalCount 和 InstanceStatusSet 均为 DescribeInstancesStatus 接口定义的字段，由于调用请求的用户暂时还没有云服务器实例，因此 TotalCount 在此情况下的返回值为 0， InstanceStatusSet 列表为空。

错误返回结果

若调用失败，其返回值示例如下为：

```
{
"Response": {
"Error": {
"Code": "AuthFailure.SignatureFailure",
"Message": "The provided credentials could not be validated. Please check your signature is correct."
},
"RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
}
}
```

- Error 的出现代表着该请求调用失败。Error 字段连同其内部的 Code 和 Message 字段在调用失败时是必定返回的。
- Code 表示具体出错的错误码，当请求出错时可以先根据该错误码在公共错误码和当前接口对应的错误码列表里面查找对应原因和解决方案。
- Message 显示出了这个错误发生的具体原因，随着业务发展或体验优化，此文本可能会经常保持变更或更新，用户不应依赖这个返回值。
- RequestId 用于一个 API 请求的唯一标识，如果 API 出现异常，可以联系我们，并提供该 ID 来解决问题。

公共错误码 (TODO: 重复信息, 是否真的需要?)

返回结果中如果存在 Error 字段，则表示调用 API 接口失败。 Error 中的 Code 字段表示错误码，所有业务都可能出现的错误码为公共错误码，下表列出了公共错误码。

错误码	错误描述
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）。
AuthFailure.MFAFailure	MFA 错误。
AuthFailure.SecretIdNotFound	密钥不存在。
AuthFailure.SignatureExpire	签名过期。
AuthFailure.SignatureFailure	签名错误。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未 CAM 授权。
DryRunOperation	DryRun 操作，代表请求将会是成功的，只是多传了 DryRun 参数。
FailedOperation	操作失败。

错误码	错误描述
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误。
UnsupportedOperation	操作不支持。
UnsupportedProtocol	http(s)请求协议错误，只支持 GET 和 POST 请求。
UnsupportedRegion	接口不支持所传地域。

公共参数

最近更新时间: 2024-09-03 18:50:01

公共参数是用于标识用户和接口鉴权目的的参数，如非必要，在每个接口单独的接口文档中不再对这些参数进行说明，但每次请求均需要携带这些参数，才能正常发起请求。

签名方法 v3

使用 TC3-HMAC-SHA256 签名方法时，公共参数需要统一放到 HTTP Header 请求头部中，如下：

参数名称	类型	必选	描述
X-TC-Action	String	是	操作的接口名称。取值参考接口文档中输入参数公共参数 Action 的说明。例如云服务器的查询实例列表接口，取值为 DescribeInstances。
X-TC-Region	String	是	地域参数，用来标识希望操作哪个地域的数据。接口接受的地域取值参考接口文档中输入参数公共参数 Region 的说明。注意：某些接口不需要传递该参数，接口文档中会对此特别说明，此时即使传递该参数也不会生效。
X-TC-Timestamp	Integer	是	当前 UNIX 时间戳，可记录发起 API 请求的时间。例如 1529223702。注意：如果与服务器时间相差超过5分钟，会引起签名过期错误。
X-TC-Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 Version 的说明。例如云服务器的版本 2017-03-12。
Authorization	String	是	HTTP 标准身份认证头部字段，例如： TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc963176630326f1024 其中， - TC3-HMAC-SHA256：签名方法，目前固定取该值； - Credential：签名凭证，AKIDEXAMPLE 是 SecretId；Date 是 UTC 标准时间的日期，取值需要和公共参数 X-TC-Timestamp 换算的 UTC 标准时间日期一致；service为产品名，必须与调用的产品域名一致，例如cvm； - SignedHeaders：参与签名计算的头部信息，content-type 和 host 为必选头部； - Signature：签名摘要。
X-TC-Token	String	否	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token。

签名方法 v1

使用 HmacSHA1 和 HmacSHA256 签名方法时，公共参数需要统一放到请求串中，如下

参数名称	类型	必选	描述
Action	String	是	操作的接口名称。取值参考接口文档中输入参数公共参数 Action 的说明。例如云服务器的查询实例列表接口，取值为 DescribeInstances。
Region	String	是	地域参数，用来标识希望操作哪个地域的数据。接口接受的地域取值参考接口文档中输入参数公共参数 Region 的说明。注意：某些接口不需要传递该参数，接口文档中会对此特别说明，此时即使传递该参数也不会生效。
Timestamp	Integer	是	当前 UNIX 时间戳，可记录发起 API 请求的时间。例如1529223702，如果与当前时间相差过大，会引起签名过期错误。
Nonce	Integer	是	随机正整数，与 Timestamp 联合起来，用于防止重放攻击。
SecretId	String	是	在云API密钥上申请的标识身份的 SecretId，一个 SecretId 对应唯一的 SecretKey ，而 SecretKey 会用来生成请求签名 Signature。
Signature	String	是	请求签名，用来验证此次请求的合法性，需要用户根据实际的输入参数计算得出。具体计算方法参见接口鉴权文档。
Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 Version 的说明。例如云服务器的版本 2017-03-12。
SignatureMethod	String	否	签名方式，目前支持 HmacSHA256 和 HmacSHA1。只有指定此参数为 HmacSHA256 时，才使用 HmacSHA256 算法验证签名，其他情况均使用 HmacSHA1 验证签名。
Token	String	否	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token 。

地域列表

地域（Region）是指物理的数据中心的地理区域。tcecloud交付验证不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议您选择最靠近您客户的地域。

您可以通过 API接口 **查询地域列表** 查看完成的地域列表。

专家服务相关接口
可用订单详情

最近更新时间: 2024-09-03 18:50:01

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

专家服务-可用订单详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAvailableExpertServiceDetail
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
EmergencyResponse	Uint64	应急响应可用次数
EmergencyResponseBuy	Bool	是否购买过应急响应
ExpertService	ExpertServiceOrderInfo	安全管家订单
ExpertServiceBuy	Bool	是否购买过安全管家
ProtectNet	Uint64	旗舰护网可用次数
ProtectNetBuy	Bool	是否购买过旗舰护网
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InternalError.MainDBFail	
InvalidParameter	

应急响应列表

最近更新时间: 2024-09-03 18:50:01

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

专家服务-应急响应列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeEmergencyResponseList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序字段 StartTime，EndTime
Filters	否	否	Array of Filters	过滤条件。 - Keyword- String - 是否必填：否 - 关键词过滤， - Uuids - String - 是否必填：否 - 主机id过滤
Limit	否	否	Uint64	需要返回的数量，最大值为100
Offset	否	否	Uint64	排序步长
Order	否	否	String	排序方法

3. 输出参数

参数名称	类型	描述
List	EmergencyResponseInfo	应急响应列表
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

安全管家列表

最近更新时间: 2024-09-03 18:50:01

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

专家服务-安全管家列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeExpertServiceList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序字段 StartTime，EndTime
Filters	否	否	Array of Filters	过滤条件。 - Keyword- String - 是否必填：否 - 关键词过滤， - Uuids - String - 是否必填：否 - 主机id过滤
Limit	否	否	Uint64	需要返回的数量，最大值为100
Offset	否	否	Uint64	排序步长
Order	否	否	String	排序方法

3. 输出参数

参数名称	类型	描述
List	SecurityButlerInfo	安全管家数据
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

专家服务订单列表

最近更新时间: 2024-09-03 18:50:01

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

专家服务-专家服务订单列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeExpertServiceOrderList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	InquireType- String - 是否必填：否 - 订单类型过滤，
Limit	否	否	Uint64	分页条数 最大100条
Offset	否	否	Uint64	分页步长

3. 输出参数

参数名称	类型	描述
List	ExpertServiceOrderInfo	订单列表
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

安全管家月巡检报告下载

最近更新时间: 2024-09-03 18:50:01

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

专家服务-安全管家月巡检报告下载

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMonthInspectionReport
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	是	否	Uint64	分页大小
Offset	是	否	Uint64	分页步长

3. 输出参数

参数名称	类型	描述
List	MonthInspectionReport	巡检报告列表
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
ResourceInsufficient	
LimitExceeded	
OperationDenied	
InvalidParameterValue	

旗舰重保列表

最近更新时间: 2024-09-03 18:50:01

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

专家服务-旗舰重保列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeProtectNetList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序字段 StartTime，EndTime
Filters	否	否	Array of Filters	过滤条件。 - Keyword- String - 是否必填：否 - 关键词过滤， - Uuids - String - 是否必填：否 - 主机id过滤
Limit	否	否	Uint64	需要返回的数量，最大值为100
Offset	否	否	Uint64	排序步长
Order	否	否	String	排序方法

3. 输出参数

参数名称	类型	描述
List	ProtectNetInfo	安全管家数据
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

入侵检测-反弹shell相关接口
删除反弹Shell事件

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据Ids删除反弹Shell事件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteReverseShellEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组. (最大100条)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
LimitExceeded.AreaQuota	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

删除反弹Shell规则

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

删除反弹Shell规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteReverseShellRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组. (最大100条)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
LimitExceeded.AreaQuota	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter.DateRange	
InvalidParameter.RegexRuleError	
InvalidParameter.ReverShellKeyFieldAllEmpty	

错误码	描述
InvalidParameter	
InvalidParameterValue	

获取反弹Shell列表

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取反弹Shell列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-06 15:48:41。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeReverseShellEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序字段：CreateTime-发生时间
Filters	否	否	Array of Filter	过滤条件。 Keywords - String - 是否必填：否 - 关键字(主机内网IP|进程名)
Limit	否	否	Uint64	返回数量，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序

3. 输出参数

参数名称	类型	描述
List	ReverseShell	列表内容
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter	

错误码	描述
InvalidParameterValue	

获取反弹Shell规则列表

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取反弹Shell规则列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeReverseShellRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 Keywords - String - 是否必填：否 - 关键字(进程名称)
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
List	ReverseShellRule	列表内容
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
LimitExceeded.AreaQuota	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter.DateRange	
InvalidParameter.RegexRuleError	

错误码	描述
InvalidParameter	
InvalidParameterValue	

导出反弹Shell事件

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出反弹Shell事件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportReverseShellEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤参数

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载链接地址。
TaskId	String	任务id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
FailedOperation.Export	
InvalidParameter	
InvalidParameterValue	

入侵检测-密码破解相关接口
删除暴力破解记录

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (DeleteBruteAttacks) 用于删除暴力破解记录。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteBruteAttacks
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	暴力破解事件Id数组。(最大 100条)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取爆破阻断模式

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取爆破阻断模式

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBanMode
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Mode	String	阻断模式，STANDARD_MODE：标准阻断，DEEP_MODE：深度阻断
StandardModeConfig	StandardModeConfig	标准阻断模式的配置
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取阻断地域

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取阻断地域

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBanRegions
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Mode	是	否	String	阻断模式，STANDARD_MODE：标准阻断，DEEP_MODE：深度阻断

3. 输出参数

参数名称	类型	描述
RegionSet	RegionSet	地域信息列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取阻断按钮状态

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取阻断按钮状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBanStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
ShowTips	Bool	是否弹窗提示信息 false: 关闭，true: 开启
Status	Uint64	阻断开关状态 0:关闭 1:开启
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

获取阻断白名单列表

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取阻断白名单列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBanWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 Keywords - String - 是否必填：否 - 查询关键字
Limit	否	否	Uint64	返回数量，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	总记录数
WhiteList	BanWhiteListDetail	白名单列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter	

错误码	描述
InvalidParameterValue	

获取密码破解列表

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取密码破解列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-06 18:35:50。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBruteAttackList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序字段：CreateTime-首次攻击时间
Filters	否	否	Array of Filter	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - Uuid - String - 是否必填：否 - 云镜唯一Uuid - Quuid - String - 是否必填：否 - 云服务器uuid - Status - String - 是否必填：否 - 状态筛选：失败：FAILED 成功：SUCCESS - UserName - String - 是否必填：否 - UserName筛选 - SrcIp - String - 是否必填：否 - 来源ip筛选 - CreateBeginTime - String - 是否必填：否 - 首次攻击时间筛选，开始时间 - CreateEndTime - String - 是否必填：否 - 首次攻击时间筛选，结束时间 - ModifyBeginTime - String - 是否必填：否 - 最近攻击时间筛选，开始时间 - ModifyEndTime - String - 是否必填：否 - 最近攻击时间筛选，结束时间 - Banned - String - 是否必填：否 - 阻断状态筛选，多个用","分割：0-未阻断（全局ZK开关关闭），82-未阻断(非专业版)，83-未阻断(已加白名单)，1-已阻断，2-未阻断-程序异常，3-未阻断-内网攻击暂不支持阻断，4-未阻断-安平暂不支持阻断
Limit	否	否	Uint64	需要返回的数量，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序

3. 输出参数

参数名称	类型	描述
BruteAttackList	BruteAttackInfo	密码破解列表
TotalCount	Uint64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	

错误码	描述
ResourceNotFound	
InvalidParameter.DateRange	
InvalidParameter	
InvalidParameterValue	

获取爆破破解规则

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取爆破破解规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBruteAttackRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Rules	BruteAttackRuleList	爆破阻断规则列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

导出密码破解记录

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (ExportBruteAttacks) 用于导出密码破解记录成CSV文件。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportBruteAttacks
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤参数

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载链接地址。
TaskId	String	导出任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
FailedOperation.Export	
InvalidParameter	
InvalidParameterValue	

修改爆破阻断模式

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

修改爆破阻断模式

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyBanMode
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Mode	是	否	String	阻断模式，STANDARD_MODE：标准阻断，DEEP_MODE：深度阻断
Ttl	否	否	Uint64	阻断时间，用于标准阻断模式

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

设置阻断开关状态

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

设置阻断开关状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyBanStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Status	是	否	Uint64	阻断状态 0:关闭 1:开启

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameterValue	

修改暴力破解规则

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

修改暴力破解规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyBruteAttackRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Rules	是	否	Array of BruteAttackRule	暴力破解判断规则

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

不再提醒爆破阻断提示弹窗

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

不再提醒爆破阻断提示弹窗

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：StopNoticeBanTips
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

入侵检测-异常登录相关接口
删除异地登录白名单规则

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口用于删除异地登录白名单规则。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteLoginWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	白名单ID (最大 100 条)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

删除异地登录记录

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (DeleteNonlocalLoginPlaces) 用于删除异地登录记录。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteNonlocalLoginPlaces
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
DelType	否	否	String	删除异地登录事件的方式，可选值："Ids"、"Ip"、"All"，默认为Ids
Ids	否	否	Array of Uint64	异地登录事件ID数组。DelType为Ids或DelType未填时此项必填
Ip	否	否	Array of String	异地登录事件的Ip。DelType为Ip时必填
Uuid	否	否	String	主机Uuid

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
LimitExceeded.AreaQuota	
ResourceNotFound	
InvalidParameter.IllegalRequest	

错误码	描述
InvalidParameter	
InvalidParameterValue	

获取登录审计列表

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取登录审计列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-06 17:19:32。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeHostLoginList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序字段：LoginTime-发生时间
Filters	否	否	Array of Filter	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - Uuid - String - 是否必填：否 - 云镜唯一Uuid - Quuid - String - 是否必填：否 - 云服务器uuid - UserName - String - 是否必填：否 - 用户名筛选 - LoginTimeBegin - String - 是否必填：否 - 按照修改时间段筛选，开始时间 - LoginTimeEnd - String - 是否必填：否 - 按照修改时间段筛选，结束时间 - SrcIp - String - 是否必填：否 - 来源ip筛选 - Status - int - 是否必填：否 - 状态筛选1:正常登录；5：已加白,14:已处理，15：已忽略 - RiskLevel - int - 是否必填：否 - 状态筛选0:高危；1：可疑
Limit	否	否	Uint64	需要返回的数量，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序

3. 输出参数

参数名称	类型	描述
HostLoginList	HostLoginList	登录审计列表
TotalCount	Uint64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter.DateRange	
InvalidParameter	

错误码	描述
InvalidParameterValue	

获取异地登录白名单合并后列表

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取异地登录白名单合并后列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-15 10:50:58。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeLoginWhiteCombinedList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - UserName - String - 是否必填：否 - 用户名筛选 - ModifyBeginTime - String - 是否必填：否 - 按照修改时间段筛选，开始时间 - ModifyEndTime - String - 是否必填：否 - 按照修改时间段筛选，结束时间
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
LoginWhiteCombinedInfos	LoginWhiteCombinedInfo	合并后的白名单列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

获取异地登录白名单列表

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取异地登录白名单列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeLoginWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 - IpOrAlias - String - 是否必填：否 - 查询关键字 - UserName - String - 是否必填：否 - 用户名筛选 - ModifyBeginTime - String - 是否必填：否 - 按照修改时间段筛选，开始时间 - ModifyEndTime - String - 是否必填：否 - 按照修改时间段筛选，结束时间
Limit	否	否	Uint64	返回数量，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
LoginWhiteLists	LoginWhiteLists	异地登录白名单数组
TotalCount	Uint64	记录总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InvalidParameter	
InvalidParameterValue	

查询常用登录地

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

此接口（DescribeUsualLoginPlaces）用于查询常用登录地。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeUsualLoginPlaces
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Uuid	是	否	String	云镜客户端UUID

3. 输出参数

参数名称	类型	描述
UsualLoginPlaces	UsualPlace	常用登录地数组
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	
MissingParameter	
LimitExceeded.AreaQuota	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

导出异地登录记录

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (ExportNonlocalLoginPlaces) 用于导出异地登录事件记录CSV文件。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportNonlocalLoginPlaces
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	Status - int - 是否必填：否 - 状态筛选1:正常登录；2：异地登录

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载链接地址。
TaskId	String	导出任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
FailedOperation.Export	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

入侵检测-恶意请求相关接口
删除恶意请求记录

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (DeleteMaliciousRequests) 用于删除恶意请求记录。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteMaliciousRequests
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	恶意请求记录ID数组，(最大100条)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
MissingParameter	
LimitExceeded.AreaQuota	
InvalidParameter	
InvalidParameterValue	

查询恶意请求白名单列表

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询恶意请求白名单列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMaliciousRequestWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 Domain - String - 基线名称
Limit	是	否	Uint64	返回数量，默认为10，最大值为100。
Offset	是	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
List	MaliciousRequestWhiteListInfo	白名单信息列表
TotalCount	Uint64	分页查询记录总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取恶意请求列表

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

入侵检测，获取恶意请求列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-06 14:42:23。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRiskDnsList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序字段：AccessCount-请求次数。MergeTime-最近请求时间
Filters	否	否	Array of Filter	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - Url - String - 是否必填：否 - Url筛选 - Status - String - 是否必填：否 - 状态筛选0:待处理；2:信任；3:不信任 - MergeBeginTime - String - 是否必填：否 - 最近访问开始时间 - MergeEndTime - String - 是否必填：否 - 最近访问结束时间
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序

3. 输出参数

参数名称	类型	描述
RiskDnsList	RiskDnsList	恶意请求列表数组
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	

错误码	描述
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

导出下载恶意请求文件

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (ExportMaliciousRequests) 用于导出下载恶意请求文件。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportMaliciousRequests
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤参数

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载链接地址。
TaskId	String	导出任务Id，可通过ExportTasks 接口下载
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameterValue	

入侵检测-文件查杀相关接口
创建网络攻击白名单

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateNetAttackWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
DealOldEvents	否	否	Uint64	是否加白所有符合该规则的告警 ，1:处理,0:不处理
Description	否	否	String	描述
EventId	否	否	Uint64	事件id
QuuidList	否	否	Array of String	quuid 列表
Scope	是	否	Uint64	是否全部主机； 0否，1是。
SrcIp	是	否	Array of String	来源IP 单IP:1.1.1.1 IP范围:1.1.1.1-1.1.2.1 IP范围：1.1.1.0/24

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	

错误码	描述
InvalidParameterValue	

文件查杀检测

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

该接口可以对入侵检测-文件查杀扫描检测

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-03 19:52:53。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateScanMalwareSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
EnableMemShellScan	否	否	Int64	是否开启恶意进程查杀[0:未开启,1:开启]
EngineType	否	否	Uint64	1标准模式（只报严重、高危）、2增强模式（报严重、高危、中危）、3严格模式（报严重、高、中、低、提示）
HostType	是	否	Int64	服务器分类：1:专业版服务器；2:自选服务器
QuuidList	否	否	Array of String	自选服务器时生效，主机quuid的string数组
ScanPattern	是	否	Uint64	扫描模式 0 全盘扫描, 1 快速扫描
TimeoutPeriod	否	否	Uint64	超时时间单位 秒 默认3600 秒

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter.DateRange	

错误码	描述
FailedOperation.APIServerFail	
FailedOperation.NoProfessionHost	
InvalidParameter	
OperationDenied	
InvalidParameterValue	
FailedOperation	

入侵管理-终止扫描任务

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

入侵管理-终止扫描任务

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteMalwareScanTask
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter.IllegalRequest	
FailedOperation.APIServerFail	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

删除木马记录

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (DeleteMalwares) 用于删除木马记录。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteMalwares
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	木马记录ID数组 (最大100条)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameterValue	

删除网络攻击白名单

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteNetAttackWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组，最大100条。

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

查询java内存马事件列表

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询java内存马事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-04-22 09:49:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeJavaMemShellList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件：Keywords: ip或者主机名模糊查询, Type，Status精确匹配，CreateBeginTime，CreateEndTime时间段
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
List	JavaMemShellInfo	事件列表
TotalCount	Uint64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取木马列表

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

入侵检测获取木马列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-02-22 18:20:24。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMalWareList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	检测排序 CreateTime
Filters	否	否	Array of Filter	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - FilePath - String - 是否必填：否 - 路径筛选 - VirusName - String - 是否必填：否 - 描述筛选 - CreateBeginTime - String - 是否必填：否 - 创建时间筛选-开始时间 - CreateEndTime - String - 是否必填：否 - 创建时间筛选-结束时间 - Status - String - 是否必填：否 - 状态筛选 4待处理,5信任,6已隔离,10隔离中,11恢复隔离中
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式 ASC,DESC

3. 输出参数

参数名称	类型	描述
MalWareList	MalWareList	木马列表
TotalCount	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	

错误码	描述
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

获取木马文件下载地址

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取木马文件下载地址

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMalwareFile
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	Uint64	木马记录ID

3. 输出参数

参数名称	类型	描述
FileUrl	String	木马文件下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

查看恶意文件详情

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查看恶意文件详情

默认接口请求频率限制：20次/秒。

接口更新时间：2021-12-09 20:22:45。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMalwareInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	Int64	唯一ID

3. 输出参数

参数名称	类型	描述
MalwareInfo	MalwareInfo	恶意文件详情信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
FailedOperation.APIServerFail	
InvalidParameter	
InvalidParameterValue	

风险预警提示

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

打开入侵检测-恶意文件检测,弹出风险预警内容

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-03 19:53:29。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMalwareRiskWarning
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
IsCheckRisk	Bool	是否开启自动扫描：true-开启，false-未开启
IsPop	Bool	是否弹出提示 true 弹出, false不弹
List	MalwareRisk	风险文件列表信息
ProcessList	MalwareRisk	异常进程列表信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

查询定时扫描配置

最近更新时间: 2024-09-03 18:50:02

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询定时扫描配置

默认接口请求频率限制：20次/秒。

接口更新时间：2022-10-25 19:31:47。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMalwareTimingScanSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AutoIsolation	Uint64	是否自动隔离：1-是，0-否
CheckPattern	Uint64	检测模式 0 全盘检测 1快速检测
ClickTimeout	Uint64	一键扫描超时时长，如：1800秒（s）
Cycle	Uint64	周期 1每天
EnableInspiredEngine	Uint64	启发引擎 0 关闭 1开启
EnableMemShellScan	Uint64	是否开启恶意进程查杀[0:未开启,1:开启]
EnableScan	Int64	定时检测开关 0 关闭1 开启
EndTime	String	检测周期 超时结束时间
EngineType	Uint64	1标准模式（只报严重、高危）、2增强模式（报严重、高危、中危）、3严格模式（报严重、高、中、低、提示）
Id	Int64	唯一ID
IsGlobal	Uint64	是否全部服务器 1 全部 2 自选
KillProcess	Uint64	是否杀掉进程 1杀掉 0不杀掉 只有开启自动隔离才生效
MonitoringPattern	Uint64	监控模式 0 标准 1深度
QuuidList	String	自选服务器时必须 主机quuid的string数组
RealTimeMonitoring	Int64	实时监控0 关闭 1开启
StartTime	String	检测周期 开始时间
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

获取网络攻击白名单列表

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNetAttackWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序列: [CreateTime]
Filters	否	否	Array of Filter	过滤条件。
IP - String - 是否必填：否 - 主机ip查询				
SrcIP- String - 是否必填：否 - 白名单ip查询				
Limit	否	否	Uint64	返回数量，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式: [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	总记录数
WhiteList	NetAttackWhiteRule	白名单列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	

错误码	描述
InvalidParameterValue	

查询木马扫描进度

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询木马扫描进度

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeScanMalwareSchedule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
IsSchedule	Bool	是否正在扫描中
RiskFileNumber	Int64	风险文件数,当进度满了以后才有该值
ScanStatus	Uint64	0 从未扫描过、 1 扫描中、 2扫描完成、 3停止中、 4停止完成
Schedule	Int64	扫描进度（单位：%）
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

获文件查杀概览信息

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取待处理风险文件数+影响服务器数+是否试用检测+最近检测时间

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeServersAndRiskAndFirstInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AddRiskFileCount	Uint64	今日新增风险文件数
IsFirstCheck	Bool	是否试用：true-是，false-否
RiskFileCount	Uint64	风险文件数
ScanTime	String	木马最近检测时间
ServersCount	Uint64	受影响服务器台数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

导出木马记录

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (ExportMalwares) 用于导出木马记录CSV文件。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportMalwares
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序值 CreateTime
Filters	否	否	Array of Filters	过滤参数。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - FilePath - String - 是否必填：否 - 路径筛选 - VirusName - String - 是否必填：否 - 描述筛选 - CreateBeginTime - String - 是否必填：否 - 创建时间筛选-开始时间 - CreateEndTime - String - 是否必填：否 - 创建时间筛选-结束时间 - Status - String - 是否必填：否 - 状态筛选
Limit	否	否	Uint64	限制条数,默认10
Offset	否	否	Uint64	偏移量 默认0
Order	否	否	String	排序 方式 ，ASC，DESC

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载链接地址。
TaskId	String	任务id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
FailedOperation.Export	

错误码	描述
InvalidParameter	
InvalidParameterValue	
FailedOperation	

定时扫描设置

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

定时扫描设置

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-03 19:52:01。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyMalwareTimingScanSettings
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
AutoIsolation	否	否	Uint64	是否自动隔离 1隔离 0 不隔离
CheckPattern	是	否	Uint64	检测模式 0 全盘检测 1快速检测
Cycle	是	否	Uint64	扫描周期 默认每天 1
EnableInspiredEngine	否	否	Uint64	启发引擎开关 0 关闭 1开启
EnableMemShellScan	否	否	Uint64	是否开启恶意进程查杀[0:未开启,1:开启]
EnableScan	是	否	Uint64	定时检测开关 0 关闭 1开启
EndTime	是	否	String	检测周期 超时结束时间，如：04:00:00
EngineType	否	否	Uint64	1标准模式（只报严重、高危）、2增强模式（报严重、高危、中危）、3严格模式（报严重、高、中、低、提示）
IsGlobal	是	否	Uint64	是否全部服务器 1 全部 2 自选
KillProcess	否	否	Uint64	是否杀掉进程 1杀掉 0不杀掉
MonitoringPattern	是	否	Uint64	监控模式 0 标准 1深度
QuuidList	否	否	Array of String	自选服务器时必须 主机quuid的string数组
RealTimeMonitoring	是	否	Uint64	实时监控 0 关闭 1开启
StartTime	是	否	String	检测周期 开始时间，如：02:00:00

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter.DateRange	
FailedOperation.APIServerFail	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

编辑网络攻击白名单

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyNetAttackWhiteList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
DealOldEvents	是	否	Uint64	是否加白所有符合该规则的告警 ，1:处理,0:不处理
Description	否	否	String	规则描述
Id	是	否	Uint64	规则id
QuuidList	否	否	Array of String	quuid 列表
Scope	是	否	Uint64	是否全部主机； 0否，1是。
SrcIp	是	否	Array of String	来源IP 单IP:1.1.1.1 IP范围:1.1.1.1-1.1.2.1 IP范围：1.1.1.0/24

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

恢复木马文件

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口（RecoverMalwares）用于批量恢复已经被隔离的木马文件。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：RecoverMalwares
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	木马Id数组（最大100条）

3. 输出参数

参数名称	类型	描述
FailedIds	Uint64	恢复失败id数组，若无则返回空数组
SuccessIds	Uint64	恢复成功id数组，若无则返回空数组
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
FailedOperation.Recover	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

隔离木马

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口（SeparateMalwares）用于隔离木马。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SeparateMalwares
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	木马事件ID数组。(最大100条)
KillProcess	否	否	Bool	是否杀掉进程

3. 输出参数

参数名称	类型	描述
FailedIds	Uint64	隔离失败的id数组，若无则返回空数组
SuccessIds	Uint64	隔离成功的id数组，若无则返回空数组
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
FailedOperation.PartSeparate	
FailedOperation.SingleSeparate	
InvalidParameter	

错误码	描述
InvalidParameterValue	

信任木马文件

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口(TrustMalwares)将被识别木马文件设为信任。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：TrustMalwares
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	木马ID数组（单次不超过的最大条数：100）

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	
MissingParameter	
LimitExceeded.AreaQuota	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

取消信任木马

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口（UntrustMalwares）用于取消信任木马文件。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UntrustMalwares
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	木马ID数组 (最大100条)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

入侵检测-本地提权相关接口
删除本地提权事件

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据Ids删除本地提权

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeletePrivilegeEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组. (最大100条)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

删除本地提权规则

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

删除本地提权规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeletePrivilegeRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组，最大100条。

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
LimitExceeded.AreaQuota	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter.DateRange	
InvalidParameter.RegexRuleError	
InvalidParameter	

错误码	描述
InvalidParameterValue	

获取本地提权事件列表

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取本地提权事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-06 15:33:40。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribePrivilegeEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序字段：CreateTime-发现时间
Filters	否	否	Array of Filter	过滤条件。 Keywords - String - 是否必填：否 - 关键词(主机IP)
Limit	否	否	Uint64	返回数量，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序

3. 输出参数

参数名称	类型	描述
List	PrivilegeEscalationProcess	数据列表
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter	

错误码	描述
InvalidParameterValue	

获取本地提权规则列表

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取本地提权规则列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribePrivilegeRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 Keywords - String - 是否必填：否 - 关键字(进程名称)
Limit	否	否	Uint64	返回数量，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
List	PrivilegeRule	列表内容
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

导出本地提权事件

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出本地提权事件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportPrivilegeEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤参数

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载链接地址。
TaskId	String	导出任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
FailedOperation.Export	
InvalidParameter	
InvalidParameterValue	

入侵检测-高危命令相关接口
校验高危命新增用户规则参数

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

校验高危命令用户规则新增和编辑时的参数。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CheckBashRuleParams
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
CheckField	是	否	String	校验内容 Name或Rule ，两个都要校验时逗号分割
EventId	否	否	Uint64	在事件列表中新增白名时需要提交事件ID
Id	否	否	Uint64	编辑时传的规则id
Name	否	否	String	填入的规则名称
Rule	否	否	String	用户填入的正则表达式："正则表达式" 需与 "提交EventId对应的命令内容" 相匹配

3. 输出参数

参数名称	类型	描述
ErrCode	Uint64	0=校验通过 1=规则名称校验不通过 2=正则表达式校验不通过
ErrMsg	String	校验信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

错误码	描述
InvalidParameter	

删除高危命令事件

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据Ids删除高危命令事件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteBashEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组，最大100条。

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
LimitExceeded.AreaQuota	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

删除高危命令规则

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

删除高危命令规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteBashRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组，最大100条。

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
LimitExceeded.AreaQuota	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter.DateRange	
InvalidParameter.RegexRuleError	

获取高危命令列表

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取高危命令列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-06 14:53:54。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBashEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序字段：CreateTime-发生时间。ModifyTime-处理时间
Filters	否	否	Array of Filter	过滤条件。 Keywords - String - 是否必填：否 - 关键词(主机内网IP)
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序

3. 输出参数

参数名称	类型	描述
List	BashEvent	高危命令事件列表
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	

错误码	描述
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

获取高危命令列表(新)

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取高危命令列表(新)

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-19 20:56:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBashEventsNew
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序字段：CreateTime-发生时间。ModifyTime-处理时间
Filters	否	否	Array of Filter	过滤条件。 - HostName - String - 是否必填：否 - 主机名 - Hostip - String - 是否必填：否 - 主机内网IP - HostIp - String - 是否必填：否 - 主机内网IP - RuleCategory - Int - 是否必填：否 - 策略类型,全部或者单选(0:系统 1:用户) - RuleName - String - 是否必填：否 - 策略名称 - RuleLevel - Int - 是否必填：否 - 威胁等级,可以多选 - Status - Int - 是否必填：否 - 处理状态,可多选(0:待处理 1:已处理 2:已加白 3:已忽略 4:已删除 5:已拦截) - DetectBy - Int - 是否必填：否 - 数据来源,可多选(0:bash日志 1:实时监控) - StartTime - String - 是否必填：否 - 开始时间 - EndTime - String - 是否必填：否 - 结束时间
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式：根据请求次数排序：asc-升序/desc-降序

3. 输出参数

参数名称	类型	描述
List	BashEventNew	高危命令事件列表
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	

错误码	描述
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

获取高危命令规则列表

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取高危命令规则列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBashRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 Keywords - String - 是否必填：否 - 关键字(规则名称)
Limit	否	否	Uint64	返回数量，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。
Type	是	否	Uint64	0-系统规则; 1-用户规则

3. 输出参数

参数名称	类型	描述
List	BashRule	列表内容
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	

错误码	描述
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

新增或修改高危命令规则（支持多服务器选择）

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

新增或修改高危命令规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：EditBashRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
DealOldEvents	否	否	Uint64	是否处理旧事件为白名单 0=不处理 1=处理
EventId	否	否	Uint64	事件列表点击"加入白名单"时,需要传EventId 事件的id
HostIp	否	否	String	主机IP
Id	否	否	Uint64	规则ID（新增时不填）
IsGlobal	否	否	Uint64	是否全局规则(默认否)：1-全局，0-非全局
Level	否	否	Uint64	危险等级(0:无，1: 高危 2:中危 3: 低危)
Name	否	否	String	规则名称，编辑时不可修改规则名称
Rule	否	否	String	正则表达式 ，编辑时不可修改正则表达式，需要对内容QueryEscape后再base64
Uuids	否	否	Array of String	客户端ID数组
White	否	否	Uint64	0=黑名单， 1=白名单

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

错误码	描述
MissingParameter	
ResourceNotFound	
InvalidParameter.RegexRuleError	
InvalidParameter.RuleHostipErr	
InvalidParameter.IpNoValid	
InvalidParameter	
InvalidParameterValue	

导出高危命令事件

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出高危命令事件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportBashEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤参数

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载链接地址。
TaskId	String	导出任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
FailedOperation.Export	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

设置高危命令事件状态

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

设置高危命令事件状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SetBashEventsStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	ID数组，最大100条。
Status	是	否	Uint64	新状态(0-待处理 1-高危 2-正常)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.InvalidFormat	
MissingParameter	
LimitExceeded.AreaQuota	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameterValue	

切换高危命令规则状态

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

切换高危命令规则状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SwitchBashRules
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Disabled	是	否	Uint64	是否禁用
Id	是	否	Uint64	规则ID

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
LimitExceeded.AreaQuota	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter.DateRange	
InvalidParameter.RegexRuleError	

错误码	描述
InvalidParameter	
InvalidParameterValue	

其他接口

停止扫描任务

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

DeleteScanTask 该接口可以对指定类型的扫描任务进行停止扫描;

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteScanTask
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
ModuleType	是	否	String	模块类型 当前提供 Malware 木马，Vul 漏洞，Baseline 基线
QuuidList	否	否	Array of String	自选服务器时生效，主机quuid的string数组
TaskId	是	否	Uint64	任务Id

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
FailedOperation.APIServerFail	
InvalidParameter	
AuthFailure	
InvalidParameterValue	
FailedOperation	

查询资产管理环境变量列表

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询资产管理环境变量列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetEnvList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime]
Filters	否	否	Array of AssetFilters	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - Name- string - 是否必填：否 - 环境变量名 - Type- int - 是否必填：否 - 类型：0用户变量，1系统变量
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	服务器Quuid
Type	否	否	Uint64	该字段已废弃，由Filters代替
Uuid	否	否	String	服务器Uuid

3. 输出参数

参数名称	类型	描述
Envs	AssetEnvBaseInfo	列表
Total	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	

错误码	描述
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

获取客户端异常事件

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取客户端异常事件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-16 10:43:36。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeClientException
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
EndTime	否	否	String	结束时间 `2006-01-02 15:04:05` 格式
ExceptionType	是	否	Int64	客户端异常类型 1:客户端离线，2:客户端卸载
Limit	是	否	Uint64	分页单页限制数目，不为0，最大值100
Offset	是	否	Uint64	分页的偏移量
StartTime	否	否	String	起始时间 `2006-01-02 15:04:05` 格式

3. 输出参数

参数名称	类型	描述
Records	RecordInfo	事件详情
TotalCount	Uint64	事件总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

获取主机相关统计

最近更新时间: 2024-09-03 18:50:03

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取主机相关统计

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-19 10:10:24。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeGeneralStat
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
MachineRegion	否	否	String	机器所属地域。如：ap-guangzhou，ap-shanghai
MachineType	否	否	String	云主机类型。 - CVM：表示腾讯云服务器 - BM: 表示黑石物理机 - ECM: 表示边缘计算服务器 - LH: 表示轻量应用服务器 - Other: 表示混合云机器

3. 输出参数

参数名称	类型	描述
AddedOnTheFifteen	Uint64	15天内新增的主机数
AgentsAll	Uint64	主机安全客户端总数的总数
AgentsBasic	Uint64	主机安全客户端基础版的总数
AgentsOffline	Uint64	主机安全客户端 离线+关机 的总数
AgentsOnline	Uint64	主机安全客户端在线的总数
AgentsPro	Uint64	主机安全客户端专业版的总数
AgentsProExpireWithInSevenDays	Uint64	7天内到期的预付费专业版总数
FlagshipMachineCnt	Uint64	旗舰版主机数
MachinesAll	Uint64	云主机总数
MachinesUninstalled	Uint64	云主机没有安装主机安全客户端的总数
Offline	Uint64	已离线总数
ProtectDays	Uint64	保护天数
RiskMachine	Uint64	风险主机总数
Shutdown	Uint64	已关机总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取概览统计数据

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取概览统计数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeOverviewStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
BaseLineNum	Uint64	安全基线数。
BruteAttackSuccessNum	Uint64	暴力破解成功数。
MalwareNum	Uint64	木马文件数。
NonlocalLoginNum	Uint64	异地登录数。
OnlineMachineNum	Uint64	服务器在线数。
ProVersionMachineNum	Uint64	专业服务器数。
VulNum	Uint64	漏洞数。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.InvalidFormat	
MissingParameter	
InternalError.MainDBFail	

获取专业版概览信息

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

用于获取专业版概览信息。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeProVersionInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
IsAutoOpenProVersion	Bool	新增主机是否自动开通专业版
PostPayCost	Uint64	后付费昨日扣费
ProVersionNum	Uint64	开通专业版主机数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

获取专业版状态

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

用于获取单台主机或所有主机是否开通专业版状态。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeProVersionStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Uuid	是	否	String	云镜客户端UUID、填写"all"表示所有主机。

3. 输出参数

参数名称	类型	描述
Status	String	开通状态。 - UNOPENED：未开通专业版 - OPENED：已开通专业版
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

查询扫描状态

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

DescribeScanState 该接口能查询对应模块正在进行的扫描任务状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-29 09:49:27。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeScanState
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤参数; StrategyId 基线策略ID ,仅ModuleType 为 Baseline 时需要
ModuleType	是	否	String	模块类型 当前提供 Malware 木马 , Vul 漏洞 , Baseline 基线

3. 输出参数

参数名称	类型	描述
RiskEventCount	Uint64	扫描漏洞数
ScanBeginTime	String	开始扫描时间
ScanEndTime	String	扫描结束时间
ScanState	Uint64	0 从未扫描过、 1 扫描中、 2扫描完成、 3停止中、 4停止完成
Schedule	Uint64	扫描进度
TaskId	Uint64	任务Id
Type	Uint64	0一键检测 1定时检测
VulId	Uint64	任务扫描的漏洞id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter	
AuthFailure	
InvalidParameterValue	

查询扫描任务详情

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

DescribeScanTaskDetails 查询扫描任务详情，可以查询扫描进度信息/异常;

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-14 17:12:25。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeScanTaskDetails
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤参数
Limit	否	否	Uint64	需要返回的数量，最大值为100
ModuleType	是	否	String	模块类型 当前提供 Malware 木马，Vul 漏洞，Baseline 基线
Offset	否	否	Uint64	偏移量，默认为0。
TaskId	是	否	Uint64	任务ID

3. 输出参数

参数名称	类型	描述
RiskEventCount	Uint64	风险事件个数
RiskMachineCount	Uint64	发现风险机器数
ScanBeginTime	String	扫描开始时间
ScanContent	String	扫描内容
ScanEndTime	String	扫描结束时间
ScanLeftTime	Uint64	扫描剩余时间
ScanMachineCount	Uint64	扫描机器总数
ScanProgress	Uint64	扫描进度
ScanTaskDetailList	ScanTaskDetails	扫描任务信息列表
ScanTime	Uint64	检测时间
StoppingAll	Bool	任务是否全部正在被停止 ture是
TotalCount	Uint64	总数
Type	Uint64	0一键检测 1定时检测

参数名称	类型	描述
VulCount	Uint64	扫描出漏洞个数
VulInfo	VulDetailInfo	漏洞信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	
AuthFailure	
InvalidParameterValue	

查询机器扫描状态列表

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

DescribeScanTaskStatus 查询机器扫描状态列表用于过滤筛选

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeScanTaskStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
ModuleType	是	否	String	模块类型 当前提供 Malware 木马，Vul 漏洞，Baseline 基线

3. 输出参数

参数名称	类型	描述
State	TaskStatus	任务扫描状态列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter	
AuthFailure	
InvalidParameterValue	

获取安全事件动态消息

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (DescribeSecurityDynamics) 用于获取安全事件动态消息数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecurityDynamics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	返回数量，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
SecurityDynamics	SecurityDynamic	安全事件消息数组。
TotalCount	Uint64	记录总数。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.InvalidFormat	
InvalidParameter.IllegalRequest	

获取安全事件统计

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取安全事件统计

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-08 16:30:42。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecurityEventStat
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	该接口无过滤条件

3. 输出参数

参数名称	类型	描述
AttackLogsStat	EventStat	网络攻击事件统计
BaseLineTotalAffectNum	Uint64	有未处理基线安全事件的机器总数
BaselineHighStat	EventStat	高危基线漏洞事件统计
BaselineLowStat	EventStat	低危基线漏事件统计
BaselineNormalStat	EventStat	中危基线漏事件统计
BaselineRiskStat	EventStat	严重基线漏洞事件统计
BruteAttackStat	EventStat	爆破事件统计
CyberAttackTotalAffectNum	Uint64	有未处理网络攻击安全事件的机器总数
HighRiskBashStat	EventStat	高危命令事件统计
HostLoginStat	EventStat	异地事件统计
InvasionTotalAffectNum	Uint64	有未处理入侵安全事件的机器总数
MachineTotalAffectNum	Uint64	有未处理安全事件的机器总数
MaliciousRequestStat	EventStat	恶意请求事件统计
MalwareStat	EventStat	木马事件统计
PrivilegeStat	EventStat	本地提权事件统计
ReverseShellStat	EventStat	反弹Shell事件统计
Score	Uint64	安全得分

参数名称	类型	描述
VulHighStat	EventStat	高危漏洞事件统计
VulLowStat	EventStat	低危漏洞事件统计
VulNormalStat	EventStat	中危漏洞事件统计
VulRiskStat	EventStat	严重漏洞事件统计
VulStat	EventStat	漏洞数统计
VulTotalAffectNum	Uint64	有未处理漏洞安全事件的机器总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	

获取安全事件数统计数据

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取安全概览相关事件统计数据接口

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-08 16:30:42。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecurityEventsCnt
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AttackLogs	SecurityEventInfo	攻击检测相关风险事件
BaseLine	SecurityEventInfo	安全基线相关风险事件
Bash	SecurityEventInfo	高危命令相关风险事件
BruteAttack	SecurityEventInfo	密码破解相关风险事件
EffectMachineCount	Uint64	受影响机器数
EmergencyVul	SecurityEventInfo	应急漏洞相关风险事件
EventsCount	Uint64	所有事件总数
HostLogin	SecurityEventInfo	登录审计相关风险事件
LinuxVul	SecurityEventInfo	linux系统漏洞事件总数
Malware	SecurityEventInfo	木马文件相关风险事件
PrivilegeRules	SecurityEventInfo	本地提权相关风险事件
ReverseShell	SecurityEventInfo	反弹Shell相关风险事件
RiskDns	SecurityEventInfo	恶意请求相关风险事件
SysVul	SecurityEventInfo	应用漏洞风险事件
WebVul	SecurityEventInfo	Web应用漏洞相关风险事件
WindowVul	SecurityEventInfo	window 系统漏洞事件总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	
InternalError.MainDBFail	
InvalidParameter	

获取安全事件统计数据

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (DescribeSecurityTrends) 用于获取安全事件统计数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSecurityTrends
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
BeginDate	是	否	Date	开始时间，如：2021-07-10
EndDate	是	否	Date	结束时间，如：2021-07-10

3. 输出参数

参数名称	类型	描述
BaseLines	SecurityTrend	基线统计数据数组。
BruteAttacks	SecurityTrend	密码破解事件统计数据数组。
CyberAttacks	SecurityTrend	网络攻击统计数据数组。
HighRiskBashs	SecurityTrend	高危命令统计数据数组。
MaliciousRequests	SecurityTrend	恶意请求统计数据数组。
Malwares	SecurityTrend	木马事件统计数据数组。
NonLocalLoginPlaces	SecurityTrend	异地登录事件统计数据数组。
PrivilegeEscalations	SecurityTrend	本地提权统计数据数组。
ReverseShells	SecurityTrend	反弹shell统计数据数组。
Vuls	SecurityTrend	漏洞统计数据数组。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InternalError	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter.DateRange	
InvalidParameter	
InvalidParameterValue	

获取任务下发时长

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取任务下发时长

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeTaskDuration
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
TimingScan	否	否	Bool	是否定时扫描
UuidCnt	是	否	Uint64	需要执行任务的主机数

3. 输出参数

参数名称	类型	描述
Duration	Uint64	任务下发需要的时长，单位为分钟
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

获取专业版和基础版机器数

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

用于统计专业版和基础版机器数。

默认接口请求频率限制：20次/秒。

接口更新时间：2023-01-09 11:35:47。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVersionStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
BasicVersionNum	Uint64	基础版数量
GeneralVersionNum	Uint64	普惠版数量
ProVersionNum	Uint64	专业版数量
UltimateVersionNum	Uint64	旗舰版数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	
MissingParameter	
InternalError.MainDBFail	
InvalidParameter	
InvalidParameterValue	

导出扫描任务详情

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据任务id导出指定扫描任务详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportScanTaskDetails
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤参数：ipOrAlias（服务器名/ip）
ModuleType	是	否	String	模块类型，当前提供：Malware 木马，Vul 漏洞，Baseline 基线
TaskId	是	否	Uint64	本次检测的任务id（不同于出参的导出本次检测Excel的任务Id）

3. 输出参数

参数名称	类型	描述
TaskId	String	导出本次检测Excel的任务Id（不同于入参的本次检测任务id）
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

导出风险趋势

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出风险趋势

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportSecurityTrends
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
BeginDate	是	否	Date	开始时间。
EndDate	是	否	Date	结束时间。

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载链接地址。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

异步导出任务

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

用于异步导出数据量大的日志文件

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportTasks
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskId	是	否	String	任务ID

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	下载链接
Status	String	PENDING：正在生成下载链接，FINISHED：下载链接已生成，ERROR：网络异常等异常情况
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
ResourceNotFound	

修改网络攻击事件状态

最近更新时间: 2024-09-03 18:50:04

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyEventAttackStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
All	否	否	Bool	是否更新全部，即是否对所有的事件进行操作，当ids 不为空时，此参数无效
ExcludeId	否	否	Array of Uint64	排除的id
Filters	否	否	Array of Filters	过滤条件。
Type - String 攻击状态 0: 尝试攻击 1: 攻击成功 - 是否必填: 否				
Status - String 事件处理状态 0：待处理 1：已处理 2： 已加白 3： 已忽略 4：已删除 - 是否必填: 否				
SrcIP - String 来源IP - 是否必填: 否				
DstPort - String 攻击目标端口 - 是否必填: 否				
MachineName - String 主机名称 - 是否必填: 否				
InstanceID - String 主机实例ID - 是否必填: 否				
Quuids - String 主机cvm uuid - 是否必填: 否				
Ids	否	否	Array of Uint64	需要修改的事件id 数组，支持批量
Status	否	否	Uint64	0：待处理 1：已处理 2： 已加白 3： 已忽略 4：已删除

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

基线管理相关接口
修改事件忽略状态

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据检测项id或事件id批量忽略事件或取消忽略

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ChangeRuleEventsIgnoreStatus
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventIdList	否	否	Array of Uint64	事件id数组
IgnoreStatus	是	否	Uint64	忽略状态 0:取消忽略 ； 1:忽略
RuleIdList	否	否	Array of Uint64	检测项id数组

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

创建基线策略

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据策略信息创建基线策略

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateBaselineStrategy
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
CategoryIds	是	否	Array of Uint64	该策略下选择的基线id数组. 示例: [1,3,5,7]
IsGlobal	是	否	Uint64	扫描范围是否全部服务器, 1:是 0:否, 为1则为全部专业版主机
MachineType	是	否	String	云主机类型： CVM：虚拟主机 BM：裸金属 ECM：边缘计算主机 LH：轻量应用服务器 Other：混合云机器
Quuids	否	否	Array of String	主机id数组. 示例: ["quuid1","quuid2"]
RegionCode	是	否	String	主机地域. 示例: "ap-guangzhou"
ScanAt	是	否	String	定期检测时间，该时间下发扫描. 示例:“22:00”, 表示在22:00下发检测
ScanCycle	是	否	Uint64	检测周期, 表示每隔多少天进行检测.示例: 2, 表示每2天进行检测一次.
StrategyName	是	否	String	策略名称

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	

错误码	描述
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
FailedOperation.NoProfessionHost	
FailedOperation.TooManyStrategy	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

删除基线策略

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据基线策略id删除策略

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteBaselineStrategy
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
StrategyId	是	否	Uint64	基线策略id

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

基线策略概览统计数据查询

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据基线策略id查询基线策略数据概览统计

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineAnalysisData
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
StrategyId	是	否	Uint64	基线策略id

3. 输出参数

参数名称	类型	描述
IfFirstScan	Uint64	是否是第一次检测 1是 0不是
IsGlobal	Uint64	是否全部服务器：1-是 0-否
LatestScanTime	String	最后检测时间
ScanHostCount	Uint64	服务器总数
ScanRuleCount	Uint64	检测项总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
ResourceNotFound	
InvalidParameter	

错误码	描述
InvalidParameterValue	

查询基线基础信息

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询基线基础信息列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineBasicInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
BaselineName	否	否	String	基线名称

3. 输出参数

参数名称	类型	描述
BaselineBasicInfoList	BaselineBasicInfo	基线基础信息列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

查询基线详情

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据基线id查询基线详情接口

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineDetail
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
BaselineId	是	否	Uint64	基线id

3. 输出参数

参数名称	类型	描述
BaselineDetail	BaselineDetail	基线详情
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

基线影响主机列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据基线id查询基线影响主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-03-28 01:21:07。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineEffectHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
BaselineId	是	否	Uint64	基线id
Filters	否	否	Array of Filters	过滤条件。 - AliasName- String- 主机别名 - Status- Uint- 1已通过 0未通过 5检测中
Limit	是	否	Uint64	分页参数 最大100条
Offset	是	否	Uint64	分页参数
StrategyId	否	否	Uint64	策略id
UuidList	否	否	Array of String	主机uuid数组

3. 输出参数

参数名称	类型	描述
EffectHostList	BaselineEffectHost	影响服务器列表
TotalCount	Uint64	记录总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	

错误码	描述
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

服务器风险top接口

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

接口返回TopN的风险服务器

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineHostTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
StrategyId	是	否	Uint64	策略id
Top	是	否	Uint64	动态top值

3. 输出参数

参数名称	类型	描述
BaselineHostTopList	BaselineHostTopList	主机基线策略事件Top
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
FailedOperation.NoProfessionHost	
InvalidParameter	
InvalidParameterValue	

查询基线列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询基线列表信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 - StrategyId- Uint64 - 基线策略id - Status - Uint64 - 处理状态1已通过 0未通过 - Level - Uint64[] - 处理状态1已通过 0未通过 BaselineName - BaselineName - String - 基线名称 - Quuid- String - 主机quuid - Uuid- String - 主机uuid
Limit	是	否	Uint64	分页参数 最大100条
Offset	是	否	Uint64	分页参数

3. 输出参数

参数名称	类型	描述
BaselineList	BaselineInfo	基线信息列表
TotalCount	Uint64	分页查询记录总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	

错误码	描述
InvalidParameterValue	

查询基线检测项信息

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据基线id查询下属检测项信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineRule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
BaselineId	是	否	Uint64	基线id
Level	否	否	Array of Uint64	危害等级
Limit	是	否	Uint64	分页参数 最大100条
Offset	是	否	Uint64	分页参数
Quuid	否	否	String	主机quuid
Status	否	否	Uint64	状态
Uuid	否	否	String	主机uuid

3. 输出参数

参数名称	类型	描述
BaselineRuleList	BaselineRuleInfo	基线检测项列表
ShowRuleRemark	Bool	是否显示说明列：true-是，false-否
TotalCount	Uint64	分页查询记录总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	

错误码	描述
InvalidParameterValue	

基线检测进度查询

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据任务id查询基线检测进度

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineScanSchedule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskId	是	否	Uint64	任务id

3. 输出参数

参数名称	类型	描述
Schedule	Uint64	检测进度(百分比)
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

查询基线策略详情

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据基线策略id查询策略详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineStrategyDetail
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
StrategyId	是	否	Uint64	用户基线策略id

3. 输出参数

参数名称	类型	描述
CategoryIds	String	用户该策略下所有的基线id
IfScanned	Uint64	1 表示扫描过, 0没扫描过
IsGlobal	Uint64	扫描范围是否全部服务器, 1:是 0:否, 为1则为全部专业版主机
MachineType	String	云服务器类型： cvm：腾讯云服务器 bm：裸金属 ecm：边缘计算主机 lh: 轻量应用服务器 ohter: 混合云机器
PassRate	Uint64	策略扫描通过率
Quuids	String	用户该策略下的所有主机id
Region	String	主机地域
ScanAt	String	定期检测时间, 该时间下发扫描
ScanCycle	String	策略扫描周期(天)
StrategyName	String	策略名
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

错误码	描述
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

用户基线策略列表查询

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询一个用户下的基线策略信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineStrategyList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Enabled	是	否	Uint64	规则开关，1：打开 0：关闭 2:全部
Limit	是	否	Uint64	分页参数 最大100
Offset	是	否	Uint64	分页参数

3. 输出参数

参数名称	类型	描述
StrategyList	Strategy	用户策略信息列表
TotalCount	Uint64	分页查询记录的总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

基线检测项TOP

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据策略id查询基线检测项TOP

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
StrategyId	是	否	Uint64	策略id
Top	是	否	Uint64	动态top值

3. 输出参数

参数名称	类型	描述
RuleTopList	BaselineRuleTopInfo	检测项Top列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
FailedOperation.NoProfessionHost	
InvalidParameter	
InvalidParameterValue	

查询忽略检测项信息

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询已经忽略的检测项信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeIgnoreBaselineRule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	是	否	Uint64	分页参数 最大100条
Offset	是	否	Uint64	分页参数
RuleName	否	否	String	检测项名称

3. 输出参数

参数名称	类型	描述
IgnoreBaselineRuleList	IgnoreBaselineRule	忽略基线检测项列表信息
TotalCount	Uint64	分页查询记录总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

查询忽略检测项影响主机列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据检测项id与筛选条件查询忽略检测项影响主机列表信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeIgnoreRuleEffectHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 AliasName- String- 主机别名
Limit	是	否	Uint64	分页参数 最大100条
Offset	是	否	Uint64	分页参数
RuleId	是	否	Uint64	检测项id
TagNames	否	否	Array of String	主机标签名

3. 输出参数

参数名称	类型	描述
IgnoreRuleEffectHostList	IgnoreRuleEffectHostInfo	忽略检测项影响主机列表
TotalCount	Uint64	分页查询记录总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter.IllegalRequest	

错误码	描述
InvalidParameter	
InvalidParameterValue	

根据策略名查询策略是否存在

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据策略名查询策略是否存在

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:34。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeStrategyExist
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
StrategyName	是	否	String	策略名

3. 输出参数

参数名称	类型	描述
IfExist	Uint64	策略是否存在, 1是 0否
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

基线影响主机列表导出

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出基线影响主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportBaselineEffectHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
BaselineId	是	否	Uint64	基线id
BaselineName	否	否	String	基线名称
Filters	否	否	Array of Filters	筛选条件 AliasName- String- 主机别名
StrategyId	否	否	Uint64	策略id
UuidList	否	否	Array of String	主机uuid数组

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	下载地址
TaskId	String	导出任务id 可通过 ExportTasks接口下载
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	

错误码	描述
InvalidParameterValue	

导出基线列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出基线列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportBaselineList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件： - StrategyId- Uint64 - 基线策略id - Status - Uint64 - 事件状态：0-未通过，1-忽略，3-通过，5-检测中 - BaselineName - String - 基线名称 - AliasName- String - 服务器名称/服务器ip - Uuid- String - 主机uuid
IfDetail	否	否	Uint64	已废弃

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载地址（已弃用）
TaskId	String	导出文件Id 可通过ExportTasks接口下载
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

已忽略基线检测项导出

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出已忽略基线检测项信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportIgnoreBaselineRule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleName	否	否	String	检测项名称

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	文件下载地址
TaskId	String	导出任务Id，可通过ExportTasks 接口下载
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

忽略检测项影响主机列表导出

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据检测项id导出忽略检测项影响主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportIgnoreRuleEffectHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 AliasName- String- 主机别名
RuleId	是	否	Uint64	检测项id

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载地址
TaskId	String	导出任务Id，可通过ExportTasks 接口下载
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

更新基线策略信息

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据基线策略id更新策略信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UpdateBaselineStrategy
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
CategoryIds	是	否	Array of String	该策略下选择的基线id数组
IsGlobal	是	否	Uint64	扫描范围是否全部服务器, 1:是 0:否, 为1则为全部专业版主机
MachineType	是	否	String	云主机类型： cvm：腾讯云服务器 bm：裸金属 ecm：边缘计算主机 lh:轻量应用服务器 other:混合云机器
Quuids	是	否	Array of String	主机id数组
RegionCode	是	否	String	主机地域 ap-guangzhou
ScanAt	是	否	String	定期检测时间，该时间下发扫描
ScanCycle	是	否	Uint64	检测周期
StrategyId	是	否	Uint64	策略id
StrategyName	是	否	String	策略名称

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	

错误码	描述
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter.IllegalRequest	
FailedOperation.NoProfessionHost	
InvalidParameter	
InvalidParameterValue	

安全运营相关接口
添加历史搜索记录

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

添加历史搜索记录

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateSearchLog
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
SearchContent	是	否	String	搜索内容

3. 输出参数

参数名称	类型	描述
Status	Uint64	0：成功，非0：失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

添加检索模板

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

添加检索模板

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-09 16:57:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateSearchTemplate
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
SearchTemplate	是	否	SearchTemplate	搜索模板

3. 输出参数

参数名称	类型	描述
Status	Uint64	0：成功，非0：失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	
InvalidParameter.NameHasRepetition	

删除检索模板

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

删除检索模板

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-09 16:57:46。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteSearchTemplate
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	Uint64	模板ID

3. 输出参数

参数名称	类型	描述
Status	Uint64	0：成功，非0：失败
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

获取ES字段聚合结果

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取ES字段聚合结果

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeESAggregations
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Query	是	否	String	ES聚合条件JSON

3. 输出参数

参数名称	类型	描述
Data	String	ES聚合结果JSON
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
FailedOperation.APIServerFail	
InvalidParameter	
InvalidParameterValue	

查询日志检索服务信息

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询日志检索服务信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-09 16:53:15。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeHistoryService
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
BuyStatus	Uint64	1 可购买 2 只能升降配 3 只能跳到续费管理页
EndTime	String	到期时间
InquireNum	Uint64	用户已购容量 单位 G
IsAutoOpenRenew	Uint64	是否自动续费,0 初始值, 1 开通 2 没开通
ResourceId	String	资源ID
StartTime	String	开始时间
Status	Uint64	0 没开通 1 正常 2隔离 3销毁
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

获取索引列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取索引列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeIndexList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Data	String	ES 索引信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
FailedOperation.APIServerFail	

获取日志检索容量使用统计

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取日志检索容量使用统计

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-09 16:52:41。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeLogStorageStatistic
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
TotalSize	Uint64	总容量（单位：GB）
UsedSize	Uint64	已使用容量（单位：GB）
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

导出ES查询文档列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出ES查询文档列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSearchExportList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Query	是	否	String	ES查询条件JSON

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	下载地址
TaskId	Uint64	导出的任务号
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取历史搜索记录

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取历史搜索记录

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-09 16:57:07。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSearchLogs
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Data	String	历史搜索记录 保留最新的10条
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

获取快速检索列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取快速检索列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-09 16:57:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSearchTemplates
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
List	SearchTemplate	模板列表
TotalCount	Uint64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

新版基线管理相关接口
删除基线策略配置

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

删除基线策略配置

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:02:51。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteBaselinePolicy
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
PolicyIds	是	否	Array of Int64	策略Id

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

删除基线规则

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

删除基线规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:02:34。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteBaselineRule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleId	是	否	Int64	规则Id

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
FailedOperation	

删除基线忽略规则

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

删除基线忽略规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 11:59:19。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteBaselineRuleIgnore
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
RuleIds	是	否	Array of Int64	规则Id

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

删除基线弱口令

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

删除基线弱口令

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:32:04。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteBaselineWeakPassword
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
PasswordIds	是	否	Array of Int64	弱口令Id

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

获取基线检测详情记录

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线检测详情记录

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:34:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序列: [HostCount|StartTime|StopTime]
Filters	否	否	Array of Filter	- PolicyName - string - 是否必填：否 - 策略名称 - PolicyDetectStatus - int - 是否必填：否 - 1:检测中 2:检测完成 - FirstTime - string - 是否必填：否 - 开始时间 - LastTime - string - 是否必填：否 - 结束时间
Limit	否	否	Int64	限制条数,默认10,最大100
Offset	否	否	Int64	偏移量,默认0
Order	否	否	String	排序方式: [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
List	BaselinePolicyDetect	无
Total	Int64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
FailedOperation	

获取基线检测概览

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线检测概览

默认接口请求频率限制：20次/秒。

接口更新时间：2022-10-25 10:23:03。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineDetectOverview
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
PolicyId	否	否	Int64	策略Id

3. 输出参数

参数名称	类型	描述
HostCount	Int64	检测服务器数
ItemCount	Int64	检测项
LatestNotPassCount	Int64	最近一次检测未通过个数
LatestPassCount	Int64	最近一次检测通过个数
PassRate	Int64	通过率*100%
PolicyCount	Int64	检测策略项
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
FailedOperation	

获取基线下载列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线下载列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:08:32。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineDownloadList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	**此参数对外不可见。** 可选排序列: [StartTime|EndTime]
Filters	否	否	Array of Filter	**此参数对外不可见。** - Status - int - 是否必填：否 - 0:导出中 1:已完成 - StartTime - string - 是否必填：否 - 开始时间 - EndTime - string - 是否必填：否 - 结束时间 - TaskName - string - 是否必填：否 - 任务名称
Limit	否	否	Int64	**此参数对外不可见。** 限制条数,默认10,最大100
Offset	否	否	Int64	**此参数对外不可见。** 偏移量,默认0
Order	否	否	String	**此参数对外不可见。** 排序方式: [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
List	BaselineDownload	无
Total	Int64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

错误码	描述
InvalidParameter	

获取基线修复列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线修复列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:08:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineFixList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	**此参数对外不可见。** 可选排序列: [CreateTime|MoifyTime|FixTime]
Filters	否	否	Array of Filter	**此参数对外不可见。** ItemName- string - 是否必填：否 - 项名称
Limit	否	否	Int64	**此参数对外不可见。** 限制条数,默认10,最大100
Offset	否	否	Int64	**此参数对外不可见。** 偏移量,默认0
Order	否	否	String	**此参数对外不可见。** 排序方式: [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
List	BaselineFix	无
Total	Int64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

获取基线检测主机列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线检测主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:36:16。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineHostDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序列: [LastTime|ItemCount|PassedItemCount|NotPassedItemCount|FirstTime]
Filters	否	否	Array of Filter	- PolicyId - int64 - 是否必填：否 - 策略Id - HostName - string - 是否必填：否 - 主机名称</i> - HostIp - string - 是否必填：否 - 主机Ip</i> - ItemId - int64 - 是否必填：否 - 项Id</i> - RuleId - int64 - 是否必填：否 - 规则Id - DetectStatus - int - 是否必填：否 - 检测状态 - Level - int - 是否必填：否 - 风险等级 - StartTime - string - 是否必填：否 - 开时时间 - EndTime - string - 是否必填：否 - 结束时间
Limit	否	否	Int64	限制条数,默认10,最大100
Offset	否	否	Int64	偏移量,默认0
Order	否	否	String	排序方式: [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
List	BaselineHostDetect	无
Total	Int64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
FailedOperation	

获取忽略规则主机列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取忽略规则主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:28:44。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineHostIgnoreList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Int64	限制条数,默认10,最大100
Offset	否	否	Int64	偏移量,默认0
RuleID	是	否	Int64	请求的规则

3. 输出参数

参数名称	类型	描述
List	BaselineHost	无
Total	Int64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

获取基线服务器风险TOP5

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线服务器风险TOP5

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 11:55:23。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineHostRiskTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
PolicyId	否	否	Int64	策略ID

3. 输出参数

参数名称	类型	描述
HostRiskTop5	HostRiskLevelCount	风险主机top5
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
FailedOperation	

获取基线检测项的列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线检测项的列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-10-13 10:14:09。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineItemDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序列: [HostCount|FirstTime|LastTime]
Filters	否	否	Array of Filter	- HostId - string - 是否必填：否 - 主机Id - RuleId - int64 - 是否必填：否 - 规则Id - PolicyId - int64 - 是否必填：否 - 规则Id - ItemName - string - 是否必填：否 - 项名称 - DetectStatus - int - 是否必填：否 - 检测状态 - Level - int - 是否必填：否 - 风险等级 - StartTime - string - 是否必填：否 - 开始时间 - EndTime - string - 是否必填：否 - 结束时间
Limit	否	否	Int64	限制条数,默认10,最大100
Offset	否	否	Int64	偏移量,默认0
Order	否	否	String	排序方式: [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
List	BaselineItemDetect	无
Total	Int64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
FailedOperation	

获取忽略规则项列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取忽略规则项列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:03:58。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineItemIgnoreList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	**此参数对外不可见。** 可选排序列 [ID]
Filters	否	否	Array of Filter	**此参数对外不可见。** CatgoryId - int64 - 是否必填：否 - 规则Id
Limit	否	否	Int64	**此参数对外不可见。** 限制条数,默认10,最大100
Offset	否	否	Int64	**此参数对外不可见。** 请求偏移默认0
Order	否	否	String	**此参数对外不可见。** 排序方式 [ASC:升序|DESC:降序]
RuleID	是	否	Int64	**此参数对外不可见。** 忽略规则ID

3. 输出参数

参数名称	类型	描述
List	BaselineItemInfo	无
Total	Int64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

错误码	描述
InvalidParameter	

获取基线检测项信息

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线检测项信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:38:03。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineItemInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序列
Filters	否	否	Array of Filter	- ItemId - int64 - 是否必填：否 - 项Id</i> - PolicyId - int64 - 是否必填：否 - 项Id</i> - Level - int - 是否必填：否 - 风险等级 - ItemName - string - 是否必填：否 - 检测项名字 - RuleId - int - 是否必填：否 - 规则Id
Limit	否	否	Int64	限制条数,默认10,最大100
Offset	否	否	Int64	偏移量,默认0
Order	否	否	String	排序方式: [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
List	BaselineItemInfo	结果列表
Total	Int64	总条目数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

获取基线项检测结果列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线项检测结果列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-10-13 10:13:14。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineItemList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序列
Filters	否	否	Array of Filter	- PolicyId - int64 - 是否必填：否 - 策略Id - RuleId - int64 - 是否必填：否 - 规则Id - HostId - string - 是否必填：否 - 主机Id - HostName - string - 是否必填：否 - 主机名 - HostIp - string - 是否必填：否 - 主机IP - ItemId - String - 是否必填：否 - 检测项Id - ItemName - String - 是否必填：否 - 项名称 - DetectStatus - int - 是否必填：否 - 检测状态[0:未通过|3:通过|5:检测中] - Level - int - 是否必填：否 - 风险等级 - StartTime - string - 是否必填：否 - 开始时间 - EndTime - string - 是否必填：否 - 结束时间
Limit	否	否	Int64	限制条数,默认10,最大100
Offset	否	否	Int64	偏移量,默认0
Order	否	否	String	排序方式: [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
List	BaselineItem	无
Total	Int64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

获取基线检测项TOP5

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线检测项TOP5

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:35:07。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineItemRiskTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
PolicyId	否	否	Int64	策略ID

3. 输出参数

参数名称	类型	描述
RiskItemTop5	BaselineRiskItem	结果数组
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
FailedOperation	

获取基线策略列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线策略列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:03:23。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselinePolicyList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序列: [RuleCount|ItemCount|HostCount]
Filters	否	否	Array of Filter	PolicyName - String - 是否必填：否 - 策略名称
Limit	否	否	Int64	限制条数,默认10,最大100
Offset	否	否	Int64	偏移量,默认0
Order	否	否	String	排序方式: [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
List	BaselinePolicy	无
Total	Int64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

获取基线分类列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线分类列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:22:40。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineRuleCategoryList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
List	BaselineCategory	无
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

获取基线规则检测列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线规则检测列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:35:47。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineRuleDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序列: [HostCount|FirstTime|LastTime]
Filters	否	否	Array of Filter	- PolicyId - int64 - 是否必填：否 - 策略Id - ItemId - int64 - 是否必填：否 - 策略Id - RuleName - string - 是否必填：否 - 规则名称 - DetectStatus - int - 是否必填：否 - 检测状态 - StartTime - string - 是否必填：否 - 开时时间 - EndTime - string - 是否必填：否 - 结束时间
Limit	否	否	Int64	限制条数,默认10,最大100
Offset	否	否	Int64	偏移量,默认0
Order	否	否	String	排序方式: [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
List	BaselineRuleDetect	无
Total	Int64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

获取基线忽略规则列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线忽略规则列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-24 13:37:14。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineRuleIgnoreList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序列: [HostCount]
Filters	否	否	Array of Filter	- RuleName - String - 是否必填：否 - 规则名称 - ItemId- int - 是否必填：否 - 检测项Id
Limit	否	否	Int64	限制条数,默认10,最大100
Offset	否	否	Int64	偏移量,默认0
Order	否	否	String	排序方式: [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
List	BaselineRule	列表
Total	Int64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

获取基线规则列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线规则列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:03:09。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineRuleList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序列
Filters	否	否	Array of Filter	- RuleName - String - 是否必填：否 - 规则名称 - CategoryId - int64 - 是否必填：否 自定义筛选为-1 - 规则分类 - RuleType - int - 是否必填：否 0:系统 1:自定义 - 规则类型
Limit	否	否	Int64	限制条数,默认10,最大100
Offset	否	否	Int64	偏移量,默认0
Order	否	否	String	排序方式: [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
List	BaselineRule	无
Total	Int64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

获取基线弱口令列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取基线弱口令列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:29:50。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeBaselineWeakPasswordList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序列 [CreateTime|ModifyTime]
Filters	否	否	Array of Filter	WeakPassword - string - 是否必填：否 - 弱口令
Limit	否	否	Int64	限制条数,默认10,最大100
Offset	否	否	Int64	偏移量,默认0
Order	否	否	String	排序方式 [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
List	BaselineWeakPassword	无
Total	Int64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

获取全网热点漏洞

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取全网热点漏洞

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeHotVulTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
List	VulStoreListInfo	漏洞信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

获取一键忽略受影响的检测项和主机信息

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取一键忽略受影响的检测项和主机信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:05:46。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeIgnoreHostAndItemConfig
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	- ItemId - int64 - 是否必填：否 - 项Id</i> - RuleId - int64 - 是否必填：否 - 规则Id - HostId - string - 是否必填：否 - 主机Id

3. 输出参数

参数名称	类型	描述
HostSet	BaselineHost	受影响主机
ItemSet	BaselineItemInfo	受影响检测项
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

获取漏洞库列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取漏洞库列表

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulStoreList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序列: [PublishDate]
Filters	否	否	Array of Filter	
VulName- string - 是否必填：否 - 漏洞名称				
CveId- string - 是否必填：否 - cveid				
VulCategory- string - 是否必填：否 - 漏洞分类 1 Web-CMS漏洞 ,2 应用漏洞 ,4 Linux软件漏洞,5 Windows系统漏洞				
Method- string - 是否必填：否 - 检测方法 0版本对比,1 poc检测				
SupportDefense- string - 是否必填：否 - 是否支持防御 0不支持,1支持				
FixSwitch- string - 是否必填：否 - 是否支持自动修复 0不支持,1支持				
Limit	否	否	Int64	限制条数,默认10,最大100
Offset	否	否	Int64	偏移量,默认0
Order	否	否	String	排序方式: [ASC:升序|DESC:降序]

3. 输出参数

参数名称	类型	描述
FreeSearchTimes	Uint64	免费搜索次数
List	VulStoreListInfo	漏洞信息
Remaining	Uint64	今日剩余搜索此时

参数名称	类型	描述
TotalCount	Uint64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

导出修复列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出修复列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:29:02。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportBaselineFixList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
ExportAll	否	否	Int64	0:过滤的结果导出；1:全部导出
Filters	否	否	Array of Filter	ItemName - String - 是否必填：否 - 项名称

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

导出基线主机检测

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出基线主机检测

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:36:37。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportBaselineHostDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
ExportAll	否	否	Int64	0:过滤的结果导出；1:全部导出
Filters	否	否	Array of Filter	- HostTag - string - 是否必填：否 - 主机标签</i> - ItemId - int64 - 是否必填：否 - 项Id</i> - RuleId - int64 - 是否必填：否 - 规则Id - IsPassed - int - 是否必填：否 - 是否通过 - RiskTier - int - 是否必填：否 - 风险等级

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

导出基线检测项

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出基线检测项

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:37:19。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportBaselineItemDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
ExportAll	否	否	Int64	0:过滤的结果导出；1:全部导出
Filters	否	否	Array of Filter	- HostId - string - 是否必填：否 - 主机Id</i> - RuleId - int64 - 是否必填：否 - 规则Id</i> - IsPassed - int - 是否必填：否 - 是否通过 - RiskTier - int - 是否必填：否 - 风险等级

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

导出检测项结果列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出检测项结果列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:38:58。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportBaselineItemList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
ExportAll	否	否	Int64	0:过滤的结果导出；1:全部导出
Filters	否	否	Array of Filter	- PolicyId - int64 - 是否必填：否 - 策略Id - RuleId - int64 - 是否必填：否 - 规则Id - HostId - string - 是否必填：否 - 主机Id - HostName - string - 是否必填：否 - 主机名 - HostIp - string - 是否必填：否 - 主机IP - ItemId - String - 是否必填：否 - 检测项Id - ItemName - String - 是否必填：否 - 项名称 - DetectStatus - int - 是否必填：否 - 检测状态[0:未通过|3:通过|5:检测中] - Level - int - 是否必填：否 - 风险等级 - StartTime - string - 是否必填：否 - 开时时间 - EndTime - string - 是否必填：否 - 结束时间

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

导出基线检测规则

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出基线检测规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:36:56。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportBaselineRuleDetectList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
ExportAll	否	否	Int64	0:过滤的结果导出；1:全部导出
Filters	否	否	Array of Filter	- RuleName - string - 是否必填：否 - 规则名称</i> - IsPassed - int - 是否必填：否 - 是否通过 - RiskTier - int - 是否必填：否 - 风险等级

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

导出弱口令配置列表

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出弱口令配置列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:05:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportBaselineWeakPasswordList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
ExportAll	否	否	Int64	0:过滤的结果导出；1:全部导出
Filters	否	否	Array of Filter	WeakPassword - string - 是否必填：否 - 弱口令

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

修复基线检测

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

修复基线检测

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:05:58。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：FixBaselineDetect
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Data	否	否	Array of String	修复内容
HostId	是	否	String	主机Id
ItemId	是	否	Int64	项Id

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
FailedOperation	

修改或新增基线策略设置

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

更改基线策略设置

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:07:43。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyBaselinePolicy
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Data	是	否	BaselinePolicy	**此参数对外不可见。** 无
Filters	否	否	Array of Filter	**此参数对外不可见。** - RuleName - String - 是否必填：否 - 规则名称 - CategoryId - int64 - 是否必填：否 自定义筛选为-1 - 规则分类 - RuleType - int - 是否必填：否 0:系统 1:自定义 - 规则类型
SelectAll	否	否	Int64	**此参数对外不可见。** 是否按照过滤的全选

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
FailedOperation	

修改或新增基线策略状态

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

更改基线策略状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-17 16:05:09。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyBaselinePolicyState
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
IsEnabled	是	否	Int64	**此参数对外不可见。** 开启状态[1:开启|0:未开启]
PolicyId	是	否	Int64	**此参数对外不可见。** 策略Id

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

修改或新增基线检测规则

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

更改基线检测规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:06:12。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyBaselineRule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Data	是	否	BaselineRule	**此参数对外不可见。** 无
Filters	否	否	Array of Filter	**此参数对外不可见。** ItemName - string - 是否必填：否 - 项名称
SelectAll	否	否	Int64	**此参数对外不可见。** 是否过滤全选

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
FailedOperation	

修改或新增基线忽略规则

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

更改基线忽略规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 12:06:22。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyBaselineRuleIgnore
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
AssetType	是	否	Int64	**此参数对外不可见。** 资产类型[0:所有专业版旗舰版|1:id|2:ip]
Filters	否	否	Array of Filter	**此参数对外不可见。** ItemName - string - 是否必填：否 - 项名称
HostIds	否	否	Array of String	**此参数对外不可见。** 主机Id
HostIps	否	否	Array of String	**此参数对外不可见。** 主机Ip
ItemIds	否	否	Array of Int64	**此参数对外不可见。** 关联项
RuleId	否	否	Int64	**此参数对外不可见。** 规则Id
RuleName	是	否	String	**此参数对外不可见。** 规则名称
SelectAll	否	否	Int64	**此参数对外不可见。** 是否全选过滤

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InternalError	
InvalidParameter	
FailedOperation	

修改或新增弱口令

最近更新时间: 2024-09-03 18:50:05

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

更改或新增弱口令

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:30:52。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyBaselineWeakPassword
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Data	是	否	Array of BaselineWeakPassword	**此参数对外不可见。** 无

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

检测基线

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

检测基线

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:33:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：StartBaselineDetect
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Param	是	否	BaselineDetectParam	基线检测参数

3. 输出参数

参数名称	类型	描述
TaskId	Int64	扫描任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	
FailedOperation	

停止基线检测

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

停止基线检测

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:33:39。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：StopBaselineDetect
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskIds	是	否	Array of Int64	取消任务ID集合

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter	

同步基线检测进度概要

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

同步基线检测进度概要

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-23 15:34:11。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SyncBaselineDetectSummary
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
DetectingTaskIds	Int64	正在检测的任务ID
EndTime	String	结束时间
HostCount	Int64	主机总数
LeftMins	Int64	扫描中剩余时间(分钟)
NotPassPolicyCount	Int64	未通过策略总数
ProgressRate	Int64	处理进度
StartTime	String	开始时间
WillFirstScan	Int64	1:即将进行首次扫描 0:已经扫描过了
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
FailedOperation	

漏洞管理相关接口
取消漏洞忽略

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

取消漏洞忽略

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:58:05。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CancelIgnoreVul
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventIds	是	否	String	漏洞事件id串，多个用英文逗号分隔

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

应急漏洞扫描

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

创建应急漏洞扫描任务

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateEmergencyVulScan
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
TimeoutPeriod	否	否	Uint64	扫描超时时长 ，单位秒
Uuids	否	否	Array of String	自选服务器时生效，主机uuid的string数组
VulId	是	否	Uint64	漏洞id

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter	
OperationDenied	

错误码	描述
InvalidParameterValue	

应急漏洞列表

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取应急漏洞列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 15:57:44。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeEmergencyVulList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序字段 PublishDate LastScanTime HostCount
Filters	否	否	Array of Filters	过滤条件。 - Status - String - 是否必填：是 - 漏洞状态筛选，0//未检测 1有风险 ，2无风险 ，3 检查中展示progress - Level - String - 是否必填：否 - 漏洞等级筛选 1:低 2:中 3:高 4:提示 - VulName- String - 是否必填：否 - 漏洞名称搜索 - Uuids- String - 是否必填：否 - 主机uuid - IsSupportDefense - int- 是否必填：否 - 是否支持防御 0:不支持 1:支持
Limit	否	否	Uint64	返回数量，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式 desc，asc

3. 输出参数

参数名称	类型	描述
ExistsRisk	Bool	是否存在风险
List	EmergencyVul	漏洞列表
TotalCount	Uint64	漏洞总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

查询检测进度

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

根据taskid查询检测进度

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeScanSchedule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskId	是	否	Uint64	任务id

3. 输出参数

参数名称	类型	描述
Schedule	Uint64	检测进度
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

定期检测配置查询

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询定期检测的配置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-03-06 19:25:22。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeScanVulSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
ClickTimeout	Uint64	一键扫描超时时长，如：1800秒（s）
EnableScan	Uint64	是否开启
EndTime	String	结束时间
StartTime	String	开始时间
TimerInterval	Uint64	定期检测间隔时间（天）
TimerTime	String	定期检测时间，如：00:00
Uuids	String	为空默认扫描全部专业版、旗舰版、普惠版主机，不为空只扫描选中主机
VulCategories	String	漏洞类型：1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞
VulEmergency	Uint64	是否紧急漏洞：0-否 1-是
VulLevels	String	危害等级：1-低危；2-中危；3-高危；4-严重 (多选英文逗号分隔)
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	

错误码	描述
MissingParameter	
InternalError.MainDBFail	
InvalidParameter	
InvalidParameterValue	

获取指定漏洞分类统计数

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取漏洞管理模块指定类型的待处理漏洞数、主机数和非专业版主机数量

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeUndoVulCounts
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
IfEmergency	否	否	String	是否应急漏洞筛选, 是 : yes
VulCategory	否	否	Uint64	漏洞分类，1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞

3. 输出参数

参数名称	类型	描述
NotProfessionCount	Uint64	普通版主机数
UndoHostCount	Int64	未处理的主机数
UndoVulCount	Uint64	未处理的漏洞数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取近日指定类型的漏洞数量和主机数量

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

漏洞管理模块，获取近日指定类型的漏洞数量和主机数量

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulCountByDates
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
IfEmergency	否	否	String	是否为应急漏洞筛选 是: yes
LastDays	否	否	Array of Uint64	需要查询最近几天的数据，需要都 -1后传入
VulCategory	否	否	Uint64	漏洞的分类: 1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞

3. 输出参数

参数名称	类型	描述
HostCount	Uint64	批量获得对应天数的主机数量
VulCount	Uint64	批量获得对应天数的漏洞数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

漏洞影响主机列表

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

漏洞影响主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-07-25 15:56:07。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulEffectHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件： - AliasName - String - 主机名筛选 - TagIds - String - 主机标签id串，多个用英文用逗号分隔 - Status - String - 状态：0-待处理 1-忽略 3-已修复 5-检测中 6-修复中 8-修复失败 - Uuid - String数组 - Uuid串数组 - Version - String数组 - 付费版本数组："Flagship"-旗舰版 "PRO_VERSION"-专业版 "BASIC_VERSION"-基础版 - InstanceState - String数组 - 实例状态数组："PENDING"-创建中 "LAUNCH_FAILED"-创建失败 "RUNNING"-运行中 "STOPPED"-关机 "STARTING"-开机中 "STOPPING"-关机中 "REBOOTING"-重启中 "SHUTDOWN"-待销毁 "TERMINATING"-销毁中 "UNKNOWN"-未知（针对非腾讯云机器，且客户端离线的场景）
Limit	是	否	Uint64	分页limit 最大100
Offset	是	否	Uint64	分页Offset
VulId	是	否	Uint64	漏洞id

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	列表总数量
VulEffectHostList	VulEffectHostList	影响主机列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

获取待处理漏洞数+影响主机数

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取待处理漏洞数+影响主机数

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-27 19:13:29。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulHostCountScanTime
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
IfFirstScan	Bool	是否第一次检测
LastFixTime	String	最后一次修复漏洞的时间
ScanTime	String	扫描时间
TaskId	Uint64	运行中的任务号, 没有任务则为0
TotalVulCount	Uint64	总漏洞数
VulHostCount	Uint64	漏洞影响主机数
hadAutoFixVul	Bool	是否有支持自动修复的漏洞事件
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

获取服务器风险top列表

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取服务器风险top列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:58:32。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulHostTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
IsFollowVul	否	否	Uint64	是否仅统计重点关注漏洞 1=仅统计重点关注漏洞, 0=统计全部漏洞
Top	是	否	Uint64	获取top值，1-100
VulCategory	否	否	Uint64	1:web-cms 漏洞，2.应用漏洞 4: Linux软件漏洞 5: windows系统漏洞 6:应急漏洞，不填或者填0时返回 1，2，4，5 的总统计数据

3. 输出参数

参数名称	类型	描述
VulHostTopList	VulHostTopInfo	服务器风险top列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

漏洞详情

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

漏洞详情，带CVSS版本

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-18 10:31:53。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulInfoCvss
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
VulId	是	否	Uint64	漏洞id

3. 输出参数

参数名称	类型	描述
CVSS	String	CVSS信息
CveId	String	漏洞CVEID
CveInfo	String	cvss详情
CvssScore	Uint64	Cvss分数
CvssScoreFloat	Float	cvss 分数 浮点型
DefenseAttackCount	Uint64	已防御的攻击次数
Description	String	漏洞描述信息
FixSwitch	Int64	修复是否支持：0-windows/linux均不支持修复 ;1-windows/linux 均支持修复 ;2-仅linux支持修复;3-仅windows支持修复
Labels	String	漏洞标签 多个逗号分割
PublicDate	String	发布时间
Reference	String	参考链接
RepairPlan	String	修复方案
SuccessFixCount	Uint64	全网修复成功次数, 不支持自动修复的漏洞默认返回0
VulId	Uint64	漏洞id
VulLevel	Uint64	危害等级：1-低危；2-中危；3-高危；4-严重
VulName	String	漏洞名称
VulType	Uint64	漏洞分类 1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

查询漏洞数量等级分布统计

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

漏洞数量等级分布统计

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:59:07。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulLevelCount
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
IsFollowVul	否	否	Uint64	是否仅统计重点关注漏洞 1=仅统计重点关注漏洞, 0=统计全部漏洞
VulCategory	否	否	Uint64	1:web-cms 漏洞，2.应用漏洞 3:安全基线 4: Linux软件漏洞 5: windows系统漏洞 6:应急漏洞，不填或者填0时返回1，2，4，5 的总统计数据

3. 输出参数

参数名称	类型	描述
VulLevelList	VulLevelInfo	统计结果
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

漏洞列表

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取漏洞列表数据

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-14 18:26:56。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序字段 Level，LastTime，HostCount
Filters	否	否	Array of Filters	过滤条件。 - Status - String - 是否必填：否 - 处理状态 0 -- 待处理 1 -- 已加白 2 -- 已删除 3 - 已忽略 - ModifyTime - String - 是否必填：否 - 最近发生时间 - Uuid- String - 是否必填：否 - 主机uuid查询 - VulName- string - - VulCategory- string - 是否必填：否 - 漏洞类别 1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 - IsSupportDefense - int- 是否必填：否 - 是否支持防御 0:不支持 1:支持 - Labels- string- 是否必填：否 - 标签搜索
Limit	否	否	Uint64	返回数量，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序顺序：desc 默认asc

3. 输出参数

参数名称	类型	描述
FollowVulCount	Uint64	重点关注漏洞总数
TotalCount	Uint64	漏洞总条数
VulInfoList	VulInfoList	漏洞列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	

错误码	描述
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取漏洞top统计

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

漏洞top统计

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:58:45。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeVulTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
IsFollowVul	否	否	Uint64	是否仅统计重点关注漏洞 1=仅统计重点关注漏洞, 0=统计全部漏洞
Top	是	否	Uint64	漏洞风险服务器top，1-100
VulCategory	否	否	Uint64	1:web-cms 漏洞，2.应用漏洞 4: Linux软件漏洞 5: windows系统漏洞 6:应急漏洞，不填或者填0时返回 1，2，4，5 的总统计数据

3. 输出参数

参数名称	类型	描述
VulTopList	VulTopInfo	漏洞top列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

导出本次漏洞检测Excel

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出本次漏洞检测Excel

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:55:06。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportVulDetectionExcel
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
TaskId	是	否	Uint64	本次漏洞检测任务id（不同于出参的导出本次漏洞检测Excel的任务Id）

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载链接地址
TaskId	String	导出本次漏洞检测Excel的任务Id（不同于入参的本次漏洞检测任务id）
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

导出漏洞检测报告

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出漏洞检测报告。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportVulDetectionReport
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤参数
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
TaskId	是	否	Uint64	漏洞扫描任务id（不同于出参的导出检测报告的任务Id）

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出文件下载链接地址
TaskId	String	导出检测报告的任务Id（不同于入参的漏洞扫描任务id）
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

导出漏洞影响主机列表

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出漏洞影响主机列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:54:52。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportVulEffectHostList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 AliasName - String - 主机名筛选
VulId	是	否	Uint64	漏洞id

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	已废弃
TaskId	String	导出任务Id，可通过ExportTasks 接口下载
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
InvalidParameter.IllegalRequest	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

漏洞管理-导出漏洞列表

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

漏洞管理-导出漏洞列表

默认接口请求频率限制：20次/秒。

接口更新时间：2023-03-21 10:26:24。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportVulList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 - VulCategory - int - 是否必填：否 - 漏洞分类筛选1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 - IfEmergency - String - 是否必填：否 - 是否为应急漏洞，查询应急漏洞传:yes - Status - String - 是否必填：是 - 漏洞状态筛选，0: 待处理 1:忽略 3:已修复 5:检测中， 控制台仅处理0,1,3,5四种状态 - Level - String - 是否必填：否 - 漏洞等级筛选 1:低 2:中 3:高 4:提示 - VulName- String - 是否必填：否 - 漏洞名称搜索
IfDetail	否	否	Uint64	是否导出详情,1是 0不是

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	导出的文件下载url（已弃用！）
TaskId	String	导出文件Id 可通过ExportTasks接口下载
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

忽略漏洞

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (IgnoreImpactedHosts) 用于忽略漏洞。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-06 14:57:53。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：IgnoreImpactedHosts
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	漏洞ID数组。

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
LimitExceeded.AreaQuota	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

一键检测

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

一键检测

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ScanVul
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
HostType	是	否	Uint64	服务器分类：1:专业版服务器；2:自选服务器
QuuidList	否	否	Array of String	自选服务器时生效，主机quuid的string数组
TimeoutPeriod	否	否	Uint64	超时时长 单位秒 默认 3600 秒
VulCategories	否	否	String	漏洞类型：1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 (多选英文;分隔)
VulEmergency	否	否	Uint64	是否是应急漏洞 0 否 1 是
VulIds	否	否	Array of Uint64	需要扫描的漏洞id
VulLevels	是	否	String	危害等级：1-低危；2-中危；3-高危；4-严重 (多选英文;分隔)

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	任务id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	

错误码	描述
ResourceNotFound	
InvalidParameter.IllegalRequest	
FailedOperation.APIServerFail	
FailedOperation.NoProfessionHost	
InvalidParameter	
OperationDenied	
InvalidParameterValue	
FailedOperation	

漏洞管理-重新检测接口

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

漏洞管理-重新检测接口

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ScanVulAgain
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
EventIds	是	否	String	漏洞事件id串，多个用英文逗号分隔
Uuids	否	否	String	重新检查的机器uuid,多个逗号分隔

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
ResourceNotFound	
FailedOperation.RescanVul	
InvalidParameter.IllegalRequest	
FailedOperation.APIServerFail	
InvalidParameter	
OperationDenied	

错误码	描述
InvalidParameterValue	

定期扫描漏洞设置

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

定期扫描漏洞设置

默认接口请求频率限制：20次/秒。

接口更新时间：2023-03-06 19:25:31。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ScanVulSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
EnableScan	否	否	Uint64	**此参数对外不可见。** 是否开启扫描 1开启 0不开启
EndTime	否	否	String	**此参数对外不可见。** 扫描结束时间，如：08:00
StartTime	否	否	String	**此参数对外不可见。** 扫描开始时间，如：00:00
TimerInterval	是	否	Uint64	**此参数对外不可见。** 定期检测间隔时间（天）
TimerTime	否	否	String	**此参数对外不可见。** 定期检测时间，如：02:10:50
Uuids	否	否	Array of String	**此参数对外不可见。** 为空默认扫描全部专业版、旗舰版、普惠版主机，不为空只扫描选中主机
VulCategories	否	否	Array of Uint64	**此参数对外不可见。** 漏洞类型：1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞, 以数组方式传参[1,2]
VulEmergency	否	否	Uint64	**此参数对外不可见。** 是否是应急漏洞 0 否 1 是
VulLevels	否	否	Array of Uint64	**此参数对外不可见。** 危害等级：1-低危；2-中危；3-高危；4-严重,以数组方式传参[1,2,3]

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

错误码	描述
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

设置中心相关接口
创建授权订单

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

CreateLicenseOrder 该接口可以创建专业版/旗舰版订单 支持预付费后付费创建 后付费订单直接创建成功 预付费订单仅下单不支付,需要调用计费支付接口进行支付

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-12 15:20:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateLicenseOrder
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
AutoProtectOpenConfig	否	否	String	该字段作废
AutoRenewFlag	否	否	Bool	是否自动续费, 默认不自动续费. 该参数仅包年包月生效
BillingDefineParams	否	否	BillingDefineParams	**此参数对外不可见。** 业务自定义参数
LicenseNum	否	否	Uint64	授权数量，需要购买的数量. 默认为1
LicenseType	否	否	Uint64	授权类型, 0 专业版-按量计费, 1专业版-包年包月，2 旗舰版-包年包月 默认为0
ModifyConfig	否	否	OrderModifyObject	变配参数
ProjectId	否	否	Uint64	项目ID . 默认为0
RegionId	否	否	Uint64	购买订单地域,这里仅支持 1 广州,9 新加坡. 推荐选择广州. 新加坡地域为白名单用户购买. 默认为1
Tags	否	否	Array of Tags	标签数组, 空则表示不需要绑定标签
TimeSpan	否	否	Uint64	购买时间长度,默认1，可选值为1,2,3,4,5,6,7,8,9,10,11,12,24,36 该参数仅包年包月生效

3. 输出参数

参数名称	类型	描述
BigDealId	String	大订单号，后付费该字段空值
DealNames	String	订单号列表
ResourceIds	String	资源ID列表,预付费订单该字段空值
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
OperationDenied	
InvalidParameterValue	
FailedOperation	

删除授权记录

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

对授权管理-订单列表内已过期的订单进行删除.(删除后的订单不在统计范畴内)

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-09 10:49:46。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteLicenseRecord
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
LicenseId	是	否	Uint64	授权ID ,可以用授权订单列表获取.
LicenseType	是	否	Uint64	授权类型
ResourceId	是	否	String	资源ID

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

查看授权绑定列表

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

该接口可以获取设置中心-授权管理,某个授权下已绑定的授权机器列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-09 10:50:08。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeLicenseBindList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	Keywords 机器别名/公私IP 模糊查询
LicenseId	是	否	Uint64	授权ID
LicenseType	是	否	Uint64	授权类型
Limit	否	否	Uint64	限制条数,默认10.
Offset	否	否	Uint64	偏移量,默认0.
ResourceId	是	否	String	资源ID

3. 输出参数

参数名称	类型	描述
List	LicenseBindDetail	绑定机器列表信息
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameterValue	

查询授权绑定进度

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询授权绑定任务的进度

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:09:36。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeLicenseBindSchedule
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤参数 Status 绑定进度状态 0 进行中 1 已完成 2 失败
Limit	否	否	Uint64	限制条数,默认10.
Offset	否	否	Uint64	偏移量,默认0
TaskId	是	否	Uint64	任务ID

3. 输出参数

参数名称	类型	描述
List	LicenseBindTaskDetail	绑定任务详情
Schedule	Uint64	进度
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	

授权概览信息

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

授权管理-授权概览信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-12 15:17:14。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeLicenseGeneral
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AutoOpenStatus	Bool	自动升级开关状态,默认 false, true 开启, false 关闭
AutoRepurchaseRenewSwitch	Bool	自动加购订单是否自动续费 ,true 开启, false 关闭
AutoRepurchaseSwitch	Bool	自动加购开关, true 开启, false 关闭
AvailableFlagshipVersionLicenseCnt	Uint64	可用旗舰版授权数
AvailableLHLicenseCnt	Uint64	可用惠普版授权数
AvailableLicenseCnt	Uint64	可用授权数
AvailableProVersionLicenseCnt	Uint64	可用专业版授权数(包含后付费).
CwpVersionLicenseCnt	Uint64	普惠版总授权数(有效订单的授权数)
ExpireLicenseCnt	Uint64	已到期授权数(不包含已删除的记录)
FlagshipVersionLicenseCnt	Uint64	旗舰版总授权数(有效订单)
IsOpenStatusHistory	Bool	历史是否开通过自动升级开关
LicenseCnt	Uint64	总授权数 (包含隔离,过期等不可用状态)
NearExpiryLicenseCnt	Uint64	即将到期授权数 (15天内到期的)
NotExpiredLicenseCnt	Uint64	未到期授权数
ProVersionLicenseCnt	Uint64	专业版总授权数(有效订单)
ProtectType	String	PROVERSION_POSTPAY 专业版-后付费, PROVERSION_PREPAY 专业版-预付费, FLAGSHIP_PREPAY 旗舰版-预付费
UsedLicenseCnt	Uint64	已使用授权数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

获取授权订单列表

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取用户所有授权订单信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-12 15:20:20。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeLicenseList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	多个条件筛选时 LicenseStatus,DeadlineStatus,ResourceId,Keywords 取交集 - LicenseStatus 授权状态信息,0 未使用,1 部分使用, 2 已用完, 3 不可用 4 可使用 - BuyTime 购买时间 - LicenseType 授权类型, 0 专业版-按量计费, 1专业版-包年包月，2 旗舰版-包年包月 - DeadlineStatus 到期状态 NotExpired 未过期, Expire 已过期(包含已销毁) NearExpiry 即将到期 - ResourceId 资源ID - Keywords IP筛选 - PayMode 付费模式 0 按量计费，1 包年包月 - OrderStatus 订单状态 1 正常 2 隔离 3 销毁
Limit	否	否	Uint64	限制条数,默认10.
Offset	否	否	Uint64	偏移量,默认0.
ResourceIds	否	否	Array of String	**此参数对外不可见。** 资源ID列表筛选(与Filters.ResourceId 不能共存,同时出现则优先使用ResourceIds)
Tags	否	否	Array of Tags	标签筛选,平台标签能力,这里传入 标签键,标签值作为一个对象

3. 输出参数

参数名称	类型	描述
List	LicenseDetail	授权数列表信息
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InternalError	
InvalidParameter	
InvalidParameterValue	

更新用户告警设置

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

更新或者插入用户告警设置(该接口废弃,请调用 ModifyWarningSetting)

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSaveOrUpdateWarnings
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
WarningObjects	否	否	Array of WarningObject	告警设置的修改内容

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

获取当前用户告警列表

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取当前用户告警列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-23 11:47:34。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeWarningList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
WarningInfoList	WarningInfoObj	获取告警列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

销毁订单

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

DestroyOrder 该接口可以对资源销毁.

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-27 11:44:19。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DestroyOrder
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
LicenseType	是	否	Uint64	授权类型 0 专业版-按量计费, 1专业版-包年包月，2 旗舰版-包年包月
ResourceId	是	否	String	资源ID

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
OperationDenied	

导出授权详情

最近更新时间: 2024-09-03 18:50:06

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出授权列表对应的绑定信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-01 11:06:27。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportLicenseDetail
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
ExportMonth	否	否	String	导出月份, 该参数仅在IsHistory 时可选.
Filters	否	否	Array of Filters	多个条件筛选时 LicenseStatus,DeadlineStatus,ResourceId,Keywords 取交集 - LicenseType 授权类型, 0 专业版-按量计费, 1专业版-包年包月，2 旗舰版-包年包月 - ResourceId 资源ID
IsHistory	否	否	Bool	是否导出全部授权详情
Tags	否	否	Array of Tags	标签筛选,平台标签能力,这里传入 标签键,标签值作为一个对象

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	下载地址,该字段废弃
TaskId	Uint64	任务ID,可通过任务ID去查下载任务
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
ResourceNotFound	

设置自动开通配置

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

用于设置新增主机自动开通专业防护配置。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-12 15:15:05。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyAutoOpenProVersionConfig
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
AutoRepurchaseRenewSwitch	否	否	Uint64	自动加购的订单是否自动续费,默认0 ,0关闭, 1开启
AutoRepurchaseSwitch	否	否	Uint64	自动加购/扩容授权开关,默认 1, 0关闭, 1开启
ProtectType	否	否	String	**此参数对外不可见。** 加固防护模式 PROVERSION_POSTPAY 专业版-按量计费 PROVERSION_PREPAY 专业版-包年包月 FLAGSHIP_PREPAY 旗舰版-包年包月
Status	是	否	String	设置自动开通状态。 - CLOSE：关闭 - OPEN：打开

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

授权批量绑定

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

设置中心-授权管理 对某个授权批量绑定机器

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-27 11:43:44。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyLicenseBinds
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
IsAll	否	否	Bool	是否全部机器(当全部机器数大于当前订单可用授权数时,多余机器会被跳过)
LicenseType	是	否	Uint64	授权类型
QuuidList	否	否	Array of String	需要绑定的机器quuid列表, 当IsAll = false 时必填,反之忽略该参数. 最大长度=2000
ResourceId	是	否	String	资源ID

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

授权批量解绑

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

设置中心-授权管理 对某个授权批量解绑机器

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-27 11:43:31。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyLicenseUnBinds
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
IsAll	否	否	Bool	是否全部机器(当全部机器数大于当前订单可用授权数时,多余机器会被跳过)
IsShrink	否	否	Bool	**此参数对外不可见。** 是否自动缩容,如果授权数剩余1,则销毁订单
LicenseType	是	否	Uint64	授权类型
QuuidList	否	否	Array of String	需要绑定的机器quuid列表, 当IsAll = false 时必填,反之忽略该参数. 最大长度=100
ResourceId	是	否	String	资源ID

3. 输出参数

参数名称	类型	描述
ErrMsg	LicenseUnBindRsp	只有解绑失败的才有该值.
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

错误码	描述
FailedOperation	

编辑订单属性

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

对订单属性编辑

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-27 11:37:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyOrderAttribute
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
AttrName	是	否	String	可编辑的属性名称 ,当前支持的有: alias 资源别名
AttrValue	是	否	String	属性值
LicenseType	是	否	Uint64	授权类型 0 专业版-按量计费, 1专业版-包年包月，2 旗舰版-包年包月
ResourceId	是	否	String	资源ID

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

修改告警设置

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

修改告警设置

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-23 11:48:21。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyWarningSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
WarningObjects	是	否	Array of WarningObject	告警设置的修改内容

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

资产管理相关接口
卸载云镜客户端

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口（DeleteMachine）用于卸载云镜客户端。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-26 17:06:53。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteMachine
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Uuid	是	否	String	云镜客户端Uuid。

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
FailedOperation.MachineDelete	
InternalError.MainDBFail	
FailedOperation.APIServerFail	

错误码	描述
InvalidParameterValue	
FailedOperation	

删除服务器关联的标签

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

删除服务器关联的标签

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteMachineTag
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Rid	是	否	Uint64	关联的标签ID

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

删除标签

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

删除标签

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteTags
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	标签ID (最大100 条)

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
MissingParameter	
ResourceNotFound	
FailedOperation	

获取帐号统计列表数据

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (DescribeAccountStatistics) 用于获取帐号统计列表数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAccountStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 Username - String - 是否必填：否 - 帐号用户名
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
AccountStatistics	AccountStatistics	帐号统计列表。
TotalCount	Uint64	帐号统计列表记录总数。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

查询应用列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询应用列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetAppList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime|ProcessCount]
Filters	否	否	Array of AssetFilters	过滤条件。 - AppName- string - 是否必填：否 - 应用名搜索 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - Type - int - 是否必填：否 - 类型：仅linux 0: 全部 1: 运维 2：数据库 3：安全 4：可疑应用 5：系统架构 6：系统应用 7：WEB服务 99:其他 - OsType - uint64 - 是否必填：否 - windows/linux - Os -String 是否必填: 否 - 操作系统(DescribeMachineOsList 接口 值)
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	查询指定Quuid主机的信息

3. 输出参数

参数名称	类型	描述
Apps	AssetAppBaseInfo	应用列表
Total	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	

错误码	描述
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

获取软件关联进程列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取软件关联进程列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetAppProcessList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Name	是	否	String	App名
Offset	否	否	Uint64	偏移量，默认为0。
Quuid	是	否	String	主机Quuid
Uuid	是	否	String	主机Uuid

3. 输出参数

参数名称	类型	描述
Process	AssetAppProcessInfo	进程列表
Total	Uint64	分区总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取内核模块详情

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取内核模块详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetCoreModuleInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	String	内核模块ID
Quuid	是	否	String	服务器Quuid
Uuid	是	否	String	服务器Uuid

3. 输出参数

参数名称	类型	描述
Module	AssetCoreModuleDetail	内核模块详情
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

查询资产管理内核模块列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询资产管理内核模块列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetCoreModuleList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序依据[Size|FirstTime|ProcessCount|ModuleCount]
Filters	否	否	Array of AssetFilters	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - Name- string - 是否必填：否 - 包名 - User- string - 是否必填：否 - 用户
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	服务器Quuid
Uuid	否	否	String	服务器Uuid

3. 输出参数

参数名称	类型	描述
Modules	AssetCoreModuleBaseInfo	列表
Total	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

获取资产管理数据库详情

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取资产管理数据库详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetDatabaseInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	String	数据库ID
Quuid	是	否	String	服务器Quuid
Uuid	是	否	String	服务器Uuid

3. 输出参数

参数名称	类型	描述
Database	AssetDatabaseDetail	数据库详情
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

查询资产管理数据库列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询资产管理数据库列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetDatabaseList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime]
Filters	否	否	Array of AssetFilters	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - User- string - 是否必填是否必填：否 - 绑定IP - Port - Int - 是否必填：否 - 端口 - Name - Int - 是否必填：否 - 1:MySQL 2:Redis 3:Oracle 4:MongoDB 5:MemCache 6:PostgreSQL 7:HBase - Proto - String - 是否必填：否 - 协议：1:TCP, 2:UDP, 3:未知 - OsType - String - 是否必填： - Os -String 是否必填: 否 - 操作系统(DescribeMachineOsList 接口 值)
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	查询指定Quuid主机的信息

3. 输出参数

参数名称	类型	描述
Databases	AssetDatabaseBaseInfo	列表
Total	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	

错误码	描述
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

获取主机所有资源数量

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取主机所有资源数量

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetHostTotalCount
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Quuid	是	否	String	主机Quuid
Uuid	是	否	String	主机Uuid

3. 输出参数

参数名称	类型	描述
Types	AssetKeyVal	各项资源数量 system : 资源监控 account: 账号 port: 端口 process: 进程 app: 应用软件 database:数据库 webapp: Web应用 webframe: Web框架 webservice: Web服务 weblocation: Web站点 systempackage: 系统安装包 jar: jar包 initservice:启动服务 env: 环境变量 coremodule: 内核模块
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取资产数量概况

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取资产数量： 主机数、账号数、端口数、进程数、软件数、数据库数、Web应用数、Web框架数、Web服务数、Web站点数

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:54:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AccountCount	Uint64	账号数
AccountNewCount	Int64	账号今日新增
DatabaseCount	Uint64	数据库数
DatabaseNewCount	Int64	数据库今日新增
MachineCount	Uint64	主机数
MachineNewCount	Int64	主机今日新增
PortCount	Uint64	端口数
PortNewCount	Int64	端口今日新增
ProcessCount	Uint64	进程数
ProcessNewCount	Int64	进程今日新增
SoftwareCount	Uint64	软件数
SoftwareNewCount	Int64	软件今日新增
WebAppCount	Uint64	Web应用数
WebAppNewCount	Int64	Web应用今日新增
WebFrameCount	Uint64	Web框架数
WebFrameNewCount	Int64	Web框架今日新增
WebLocationCount	Uint64	Web站点数
WebLocationNewCount	Int64	Web站点今日新增

参数名称	类型	描述
WebServiceCount	Uint64	Web服务数
WebServiceNewCount	Int64	Web服务今日新增
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

查询资产管理启动服务列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询资产管理启动服务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetInitServiceList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime]
Filters	否	否	Array of AssetFilters	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - Name- string - 是否必填：否 - 包名 - User- string - 是否必填：否 - 用户 - Status- string - 是否必填：否 - 默认启用状态：0未启用， 1启用 仅linux - Type- string - 是否必填：否 - 类型：类型 仅windows： 1:编码器 2:IE插件 3:网络提供者 4:镜像劫持 5:LSA提供者 6:KnownDLLs 7:启动执行 8:WMI 9:计划任务 10:Winsock提供者 11:打印监控器 12:资源管理器 13:驱动服务 14:登录
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	服务器Quuid
Uuid	否	否	String	服务器Uuid

3. 输出参数

参数名称	类型	描述
Services	AssetInitServiceBaseInfo	列表
Total	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

错误码	描述
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
ResourceNotFound	

获取Jar包详情

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取Jar包详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetJarInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	String	Jar包ID
Quuid	是	否	String	服务器Quuid
Uuid	是	否	String	服务器Uuid

3. 输出参数

参数名称	类型	描述
Jar	AssetJarDetail	Jar包详情
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

查询Jar包列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询Jar包列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetJarList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime]
Filters	否	否	Array of AssetFilters	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - Name- string - 是否必填：否 - 包名 - Type- uint - 是否必填：否 - 类型 1: 应用程序 2 : 系统类库 3 : Web服务自带库 4 : 其他依赖包 - Status- string - 是否必填：否 - 是否可执行：0否，1是
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	服务器Quuid
Uuid	否	否	String	服务器Uuid

3. 输出参数

参数名称	类型	描述
Jars	AssetJarBaseInfo	应用列表
Total	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	

错误码	描述
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

获取资产管理主机资源详细信息

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取资产管理主机资源详细信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetMachineDetail
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Quuid	是	否	String	服务器Quuid
Uuid	是	否	String	服务器Uuid

3. 输出参数

参数名称	类型	描述
MachineDetail	AssetMachineDetail	主机详情
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取资源监控列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取资产指纹页面的资源监控列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetMachineList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序[FirstTime|PartitionCount]
Filters	否	否	Array of Filter	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - OsType - String - 是否必填：否 - windows或linux - CpuLoad - Int - 是否必填：否 - 0: 未知 1: 低负载 2: 中负载 3: 高负载 - DiskLoad - Int - 是否必填：否 - 0: 0%或未知 1: 0%～20% 2: 20%～50% 3: 50%～80% 4: 80%～100% - MemLoad - Int - 是否必填：否 - 0: 0%或未知 1: 0%～20% 2: 20%～50% 3: 50%～80% 4: 80%～100% - Quuid：主机Quuid - Os -String 是否必填: 否 - 操作系统(DescribeMachineOsList 接口 值)
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序

3. 输出参数

参数名称	类型	描述
Machines	AssetMachineBaseInfo	记录列表
Total	Uint64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
MissingParameter	

错误码	描述
InvalidParameter	
InvalidParameterValue	

查询资产管理计划任务列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询资产管理计划任务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetPlanTaskList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime]
Filters	否	否	Array of AssetFilters	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - User- string - 是否必填：否 - 用户 - Status- int - 是否必填：否 - 默认启用状态：0未启用， 1启用
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	服务器Quuid
Uuid	否	否	String	服务器Uuid

3. 输出参数

参数名称	类型	描述
Tasks	AssetPlanTask	列表
Total	Uint64	总数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	

错误码	描述
InvalidParameter	
InvalidParameterValue	

获取资产管理端口列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取资产管理端口列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetPortInfoList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime|StartTime]
Filters	否	否	Array of Filter	过滤条件。 - Port - uint64 - 是否必填：否 - 端口 - Ip - String - 是否必填：否 - 绑定IP - ProcessName - String - 是否必填：否 - 监听进程 - Pid - uint64 - 是否必填：否 - PID - User - String - 是否必填：否 - 运行用户 - Group - String - 是否必填：否 - 所属用户组 - Ppid - uint64 - 是否必填：否 - PPID - Proto - string - 是否必填：否 - tcp/udp或""(空字符串筛选未知状态) - OsType - uint64 - 是否必填：否 - windows/linux - RunTimeStart - String - 是否必填：否 - 运行开始时间 - RunTimeEnd - String - 是否必填：否 - 运行结束时间 - Os -String 是否必填: 否 - 操作系统(DescribeMachineOsList 接口 值)
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	查询指定Quuid主机的信息

3. 输出参数

参数名称	类型	描述
Ports	AssetPortBaseInfo	列表
Total	Uint64	记录总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	

错误码	描述
InvalidParameterValue	

获取资产管理进程列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取资产管理进程列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetProcessInfoList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序方式：[FirstTime|StartTime]
Filters	否	否	Array of Filter	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - Name - String - 是否必填：否 - 进程名 - User - String - 是否必填：否 - 进程用户 - Group - String - 是否必填：否 - 进程用户组 - Pid - uint64 - 是否必填：否 - 进程ID - Ppid - uint64 - 是否必填：否 - 父进程ID - OsType - uint64 - 是否必填：否 - windows/linux - Status - string - 是否必填：否 - 进程状态： 1:R 可执行 2:S 可中断 3:D 不可中断 4:T 暂停状态或跟踪状态 5:Z 僵尸状态 6:X 将被销毁 - RunTimeStart - String - 是否必填：否 - 运行开始时间 - RunTimeEnd - String - 是否必填：否 - 运行结束时间 - InstallByPackage - uint64 - 是否必填：否 - 是否包安装：0否，1是 - Os -String 是否必填: 否 - 操作系统(DescribeMachineOsList 接口 值)
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	查询指定Quuid主机的信息

3. 输出参数

参数名称	类型	描述
Process	AssetProcessBaseInfo	列表
Total	Uint64	记录总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
MissingParameter	

错误码	描述
InvalidParameter	
InvalidParameterValue	

获取主机概况趋势

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取主机最近趋势情况

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetRecentMachineInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
BeginDate	是	否	Date	开始时间，如：2020-09-22
EndDate	是	否	Date	结束时间，如：2020-09-22

3. 输出参数

参数名称	类型	描述
LiveList	AssetKeyVal	在线数量列表
OfflineList	AssetKeyVal	离线数量列表
RiskList	AssetKeyVal	风险数量列表
TotalList	AssetKeyVal	总数量列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter.DateRange	
UnknownParameter	

获取资产管理系统安装包列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取资产管理系统安装包列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetSystemPackageList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序方式可选：[FistTime|InstallTime:安装时间]
Filters	否	否	Array of Filter	过滤条件。 - Name - String - 是否必填：否 - 包 名 - StartTime - String - 是否必填：否 - 安装开始时间 - EndTime - String - 是否必填：否 - 安装开始时间 - Type - int - 是否必填：否 - 安装包类型： 1:rmp 2:dpkg 3:java 4:system
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc-升序 或 desc-降序。默认：desc-降序
Quuid	是	否	String	主机Quuid
Uuid	是	否	String	主机Uuid

3. 输出参数

参数名称	类型	描述
Packages	AssetSystemPackageInfo	列表
Total	Uint64	记录总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	

错误码	描述
InvalidParameter	
InvalidParameterValue	

获取主机账号详情

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取主机账号详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetUserInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Name	是	否	String	账户名
Quuid	是	否	String	云服务器UUID
Uuid	是	否	String	主机安全UUID

3. 输出参数

参数名称	类型	描述
User	AssetUserDetail	用户详细信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
InternalError.MainDBFail	

获取账号列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取账号列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetUserList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序：[FirstTime|LoginTime|PasswordChangeTime|PasswordDuaTime] PasswordLockDays
Filters	否	否	Array of Filter	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - Name - String - 是否必填：否 - 账户名（模糊匹配） - NameStrict - String - 是否必填：否 - 账户名（严格匹配） - Uid - uint64 - 是否必填：否 - Uid - Guid - uint64 - 是否必填：否 - Guid - LoginTimeStart - String - 是否必填：否 - 开始时间，如：2021-01-11 - LoginTimeEnd - String - 是否必填：否 - 结束时间，如：2021-01-11 - LoginType - uint64 - 是否必填：否 - 0-不可登录；1-只允许key登录；2只允许密码登录；3-允许key和密码 仅linux - OsType - String - 是否必填：否 - windows或linux - Status - uint64 - 是否必填：否 - 账号状态：0-禁用；1-启用 - UserType - uint64 - 是否必填：否 - 账号类型：0访客用户，1标准用户，2管理员用户 仅windows - IsDomain - uint64 - 是否必填：否 - 是否域账号：0 不是，1是 仅windows - IsRoot - uint64 - 是否必填：否 - 是否Root权限：0 不是，1是 仅linux - IsSudo - uint64 - 是否必填：否 - 是否Sudo权限：0 不是，1是 仅linux - IsSshLogin - uint64 - 是否必填：否 - 是否ssh登录：0 不是，1是 仅linux - ShellLoginStatus - uint64 - 是否必填：否 - 是否shell登录性，0不是；1是 仅linux - PasswordStatus - uint64 - 是否必填：否 - 密码状态：1正常 2即将过期 3已过期 4已锁定 仅linux - Os -String 是否必填: 否 - 操作系统(DescribeMachineOsList 接口 值)
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	查询指定Quuid主机的信息

3. 输出参数

参数名称	类型	描述
Total	Uint64	记录总数
Users	AssetUserBaseInfo	账号列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.DateRange	
InvalidParameter	
InvalidParameterValue	

获取资产管理Web应用列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取资产管理Web应用列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebAppList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序：[FirstTime|PluginCount]
Filters	否	否	Array of Filter	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - Name - String - 是否必填：否 - Domain - String - 是否必填：否 - 站点域名 - Type - int - 是否必填：否 - 服务类型： 0：全 1:Tomcat 2:Apache 3:Nginx 4:WebLogic 5:Websphere 6:JBoss 7:Jetty 8:IHS - OsType - String - 是否必填：否 - windows/linux - Os -String 是否必填: 否 - 操作系统(Describe口 值)
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	查询指定Quuid主机的信息

3. 输出参数

参数名称	类型	描述
Total	Uint64	记录总数
WebApps	AssetWebAppBaseInfo	列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	

错误码	描述
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取资产管理Web应用插件列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取资产管理Web应用插件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebAppPluginList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	String	Web应用ID
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Quuid	是	否	String	主机Quuid
Uuid	是	否	String	主机Uuid

3. 输出参数

参数名称	类型	描述
Plugins	AssetWebAppPluginInfo	列表
Total	Uint64	分区总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取资产管理Web框架列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取资产管理Web框架列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebFrameList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序：[FirstTime|JarCount]
Filters	否	否	Array of Filter	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - Name - String - 是否必填：否 - NameStrict - String - 是否必填：否 - 框架名（严格匹配） - Lang - String - 是否必填：否 - 框架语言:j String - 是否必填：否 - 服务类型： 0：全部 1:Tomcat 2:Apache 3:Nginx 4:WebLogic 5:Websphere 6:JBoss 7:WildFly 8:Je - OsType - String - 是否必填：否 - windows/linux - Os -String 是否必填: 否 - 操作系统(Describ
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	查询指定Quuid主机的信息

3. 输出参数

参数名称	类型	描述
Total	Uint64	记录总数
WebFrames	AssetWebFrameBaseInfo	列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	

错误码	描述
InvalidParameter	
InvalidParameterValue	

获取Web站点详情

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取Web站点详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebLocationInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	String	站点Id
Quuid	是	否	String	服务器Quuid
Uuid	是	否	String	服务器Uuid

3. 输出参数

参数名称	类型	描述
WebLocation	AssetWebLocationInfo	站点信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取Web站点列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取Web站点列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebLocationList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序：[FirstTime|PathCount]
Filters	否	否	Array of Filter	过滤条件。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - Name - String - 是否必填：否 - User - String - 是否必填：否 - 运行用户 - Port - uint64 - 是否必填：否 - 站点端口 - uint64 - 是否必填：否 - 站点协议：1:HTTP,2:HTTPS - ServiceType - uint64 - 是否必填：否 - 服务类型： 1:Tomcat 2：Apache 3:Nginx 4:WebLogic 5:Websphere 6:JBoss 7:WildFly 8:Jetty 9:IHS 10: - OsType - String - 是否必填：否 - windows/linux - Os -String 是否必填: 否 - 操作系统(DescribeMachineOsList 接口 值)
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	查询指定Quuid主机的信息

3. 输出参数

参数名称	类型	描述
Locations	AssetWebLocationBaseInfo	站点列表
Total	Uint64	记录总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

错误码	描述
MissingParameter	
InvalidParameter	
InvalidParameterValue	

查询资产管理Web服务列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询资产管理Web服务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebServiceInfoList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序：[FirstTime|ProcessCount]
Filters	否	否	Array of AssetFilters	过滤条件。 - User- string - 是否必填：否 - 运行用户 - Name- string - 是否必填：否 - Web服 1:Tomcat 2:Apache 3:Nginx 4:WebLogic 5:Websphere 6:JBoss 7:WildFly - OsType- string - 是否必填：否 - Windows/linux - Os -String 是否必填: 否 - 操作系统(Des
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。 IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	查询指定Quuid主机的信息

3. 输出参数

参数名称	类型	描述
Total	Uint64	总数量
WebServices	AssetWebServiceBaseInfo	列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	

错误码	描述
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

获取Web服务关联进程列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取Web服务关联进程列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAssetWebServiceProcessList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	String	Web服务ID
Limit	否	否	Uint64	需要返回的数量，默认为10，最大值为100
Offset	否	否	Uint64	偏移量，默认为0。
Quuid	是	否	String	主机Quuid
Uuid	是	否	String	主机Uuid

3. 输出参数

参数名称	类型	描述
Process	AssetAppProcessInfo	进程列表
Total	Uint64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取组件统计列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (DescribeComponentStatistics) 用于获取组件统计列表数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeComponentStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 ComponentName - String - 是否必填：否 - 组件名称
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
ComponentStatistics	ComponentStatistics	组件统计列表数据数组。
TotalCount	Uint64	组件统计列表记录总数。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

导出区域主机列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (DescribeExportMachines) 用于导出区域主机列表。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:00:52。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeExportMachines
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 - Keywords - String - 是否必填：否 - 查询关键字 - Status - String - 是否必填：否 - 客户端在线状态（OFFLINE: 离线 | ONLINE: 在线 | UNINSTALLED：未安装） - Version - String 是否必填：否 - 当前防护版本（ PRO_VERSION：专业版 | BASIC_VERSION：基础版） 每个过滤条件只支持一个值，暂不支持多个值"或"关系查询
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。
MachineRegion	是	否	String	机器所属地域。如：ap-guangzhou，ap-shanghai
MachineType	是	否	String	云主机类型。 - CVM：表示虚拟主机 - BM: 表示黑石物理机
Offset	否	否	Uint64	偏移量，默认为0。
ProjectIds	否	否	Array of Uint64	机器所属业务ID列表

3. 输出参数

参数名称	类型	描述
TaskId	String	任务id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameterValue	

获取帐号变更历史列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (DescribeHistoryAccounts) 用于获取帐号变更历史列表数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeHistoryAccounts
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 Username - String - 是否必填：否 - 帐号名
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。
Uuid	是	否	String	云镜客户端唯一Uuid。

3. 输出参数

参数名称	类型	描述
HistoryAccounts	HistoryAccount	帐号变更历史数据数组。
TotalCount	Uint64	帐号变更历史列表记录总数。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

查询批量导入机器信息

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询批量导入机器信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-06-16 12:16:37。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeImportMachineInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件： Version - String 是否必填：否 - 当前防护版本（ PRO_VERSION：专业版 | BASIC_VERSION：基础版 | Flagship：旗舰版 | ProtectedMachines：专业版+旗舰版 ） | BASIC_PROPOST_GENERAL_DISCOUNT：普惠版+专业版按量计费+基础版主机 | UnFlagship：专业版预付费+专业版后付费+基础版+普惠版
ImportType	是	否	String	批量导入的数据类型：Ip、Name、Id 三选一
IsQueryProMachine	否	否	Bool	该参数已作废.
MachineList	是	否	Array of String	服务器内网IP（默认）/ 服务器名称 / 服务器ID 数组 (最大 1000条)

3. 输出参数

参数名称	类型	描述
EffectiveMachineInfoList	EffectiveMachineInfo	有效的机器信息列表：机器名称、机器公网/内网ip、机器标签
InvalidMachineList	String	用户批量导入失败的机器列表（例如机器不存在等...）
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter	

错误码	描述
OperationDenied	
InvalidParameterValue	

获取机器详情

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口（DescribeMachineInfo）用于获取机器详细信息。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:11:35。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMachineInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Quuid	否	否	String	Quuid，Uuid 必填一项
Uuid	否	否	String	云镜客户端唯一Uuid。

3. 输出参数

参数名称	类型	描述
AgentVersion	String	agent版本号
FreeMalwaresLeft	Uint64	免费木马剩余检测数量。
FreeVulsLeft	Uint64	免费漏洞剩余检测数量。
HasAssetScan	Uint64	是否有资产扫描记录，0无，1有
InstanceId	String	CVM或BM主机唯一标识。
IsProVersion	Bool	是否开通专业版。 - true：是 - false：否
MachineIp	String	机器ip。
MachineName	String	主机名称。
MachineOs	String	操作系统。
MachineRegion	String	机器所属地域。如：ap-guangzhou，ap-shanghai
MachineStatus	String	在线状态。 - ONLINE： 在线 - OFFLINE：离线
MachineType	String	云服务器类型。 - CVM: 腾讯云服务器 - BM: 黑石物理机 - ECM: 边缘计算服务器 - LH: 轻量应用服务器 - Other: 混合云机器
MachineWanIp	String	主机外网IP。
PayMode	String	主机状态。 - POSTPAY: 表示后付费，即按量计费 - PREPAY: 表示预付费，即包年包月
ProVersionDeadline	String	专业版到期时间(仅预付费)
ProVersionOpenDate	String	专业版开通时间。
ProtectDays	Uint64	受云镜保护天数。
ProtectType	String	防护版本 BASIC_VERSION 基础版, PRO_VERSION 专业版 Flagship 旗舰版.

参数名称	类型	描述
Quuid	String	CVM或BM主机唯一Uuid。
Uuid	String	云镜客户端唯一Uuid。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
ResourceNotFound	
InvalidParameterValue	

查询机器操作系统列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询可筛选操作系统列表.

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMachineOsList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
List	OsName	操作系统列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

获取机器地域列表

最近更新时间: 2024-09-03 18:50:07

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取机器地域列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMachineRegions
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
ALL	RegionInfo	所有地域列表(包含以上所有地域)
BM	RegionInfo	BM 黑石机器地域列表
CVM	RegionInfo	CVM 云服务器地域列表
ECM	RegionInfo	ECM 边缘计算服务器地域列表
LH	RegionInfo	LH 轻量应用服务器地域列表
Other	RegionInfo	Other 混合云地域列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameterValue	

获取区域主机列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (DescribeMachines) 用于获取区域主机列表。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-10-18 17:27:47。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMachines
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 - Ips - String - 是否必填：否 - 通过ip查询 - Names - String - 是否必填：否 - 通过实例名查询 - InstanceIds - String - 是否必填：否 - 通过实例id查询 - Status - String - 是否必填：否 - 客户端在线状态（OFFLINE: 离线/关机 | ONLINE: 在线 | UNINSTALLED：未安装 | AGENT_OFFLINE 离线| AGENT_SHUTDOWN 已关机） - Version - String 是否必填：否 - 当前防护版本（ PRO_VERSION：专业版 | BASIC_VERSION：基础版 | Flagship：旗舰版 | ProtectedMachines: 专业版+旗舰版） - Risk - String 是否必填: 否 - 风险主机(yes) - Os -String 是否必填: 否 - 操作系统(DescribeMachineOsList 接口 值) 每个过滤条件只支持一个值，暂不支持多个值"或"关系查询 - Quuid - String - 是否必填: 否 - 云服务器uuid 最大100条. - AddedOnTheFifteen- String 是否必填: 否 - 是否只查询15天内新增的主机(1：是)
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。
MachineRegion	是	否	String	机器所属地域。如：ap-guangzhou，ap-shanghai
MachineType	是	否	String	机器所属专区类型 CVM 云服务器 BM 黑石 ECM 边缘计算 LH 轻量应用服务器 Other 混合云专区
Offset	否	否	Uint64	偏移量，默认为0。
ProjectIds	否	否	Array of Uint64	机器所属业务ID列表

3. 输出参数

参数名称	类型	描述
Machines	Machine	主机列表
TotalCount	Uint64	主机数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

获取端口统计列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (DescribeOpenPortStatistics) 用于获取端口统计列表。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeOpenPortStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 Port - Uint64 - 是否必填：否 - 端口号
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
OpenPortStatistics	OpenPortStatistics	端口统计数据列表
TotalCount	Uint64	端口统计列表总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

获取进程统计列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

本接口 (DescribeProcessStatistics) 用于获取进程统计列表数据。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-07-28 23:46:05。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeProcessStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 ProcessName - String - 是否必填：否 - 进程名
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
ProcessStatistics	ProcessStatistics	进程统计列表数据数组。
TotalCount	Uint64	进程统计列表记录总数。
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameterValue	

获取指定标签关联的服务器信息

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取指定标签关联的服务器信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeTagMachines
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	Uint64	标签ID

3. 输出参数

参数名称	类型	描述
List	TagMachine	列表数据
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

获取所有主机标签

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取所有主机标签

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-29 09:47:48。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeTags
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 - Keywords - String - 是否必填：否 - 查询关键字(机器名称/机器IP - Status - String - 是否必填：否 - 客户端在线状态（OFFLINE: 离线 | ONLINE: 在线 | UNINSTALLED：未安装 | SHUTDOWN 已关机） - Version - String 是否必填：否 - 当前防护版本（ PRO_VERSION：专业版 | BASIC_VERSION：基础版） - Risk - String 是否必填: 否 - 风险主机(yes) - Os -String 是否必填: 否 - 操作系统(DescribeMachineOsList 接口 值) 每个过滤条件只支持一个值，暂不支持多个值"或"关系查询
MachineRegion	否	否	String	机器所属地域。如：ap-guangzhou
MachineType	否	否	String	云主机类型。 - CVM：表示云服务器 - BM: 表示黑石物理机 - ECM: 表示边缘计算服务器 - LH: 表示轻量应用服务器 - Other: 表示混合云服务器

3. 输出参数

参数名称	类型	描述
List	Tag	列表信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	

错误码	描述
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

新增或编辑标签

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

新增或编辑标签

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：EditTags
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	否	否	Uint64	标签ID
Name	是	否	String	标签名
Quuids	否	否	Array of String	Quuid

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
MissingParameter	
LimitExceeded.AreaQuota	
ResourceNotFound	
InvalidParameterValue.TagNameLengthLimit	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

导出资产管理内核模块列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出资产管理内核模块列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportAssetCoreModuleList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序依据[FirstTime|Size|ProcessCount|ModuleCount]
Filters	否	否	Array of AssetFilters	过滤条件。 - Name- string - 是否必填：否 - 包名 - User- string - 是否必填：否 - 用户
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	服务器Quuid
Uuid	否	否	String	服务器Uuid

3. 输出参数

参数名称	类型	描述
TaskId	String	异步下载任务ID，需要配合ExportTasks接口使用
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	

错误码	描述
InvalidParameter	
InvalidParameterValue	

导出资产管理Web服务列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出资产管理Web服务列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportAssetWebServiceInfoList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	可选排序：[FirstTime|ProcessCount]
Filters	否	否	Array of AssetFilters	过滤条件。 - User- string - 是否必填：否 - 运行用户 - Name- string - 是否必填：否 - Web服 1:Tomcat 2:Apache 3:Nginx 4:WebLogic 5:Websphere 6:JBoss 7:WildFly - OsType- string - 是否必填：否 - Windows/linux
Order	否	否	String	排序方式，asc升序 或 desc降序
Quuid	否	否	String	查询指定Quuid主机的信息

3. 输出参数

参数名称	类型	描述
TaskId	String	异步下载任务ID，需要配合ExportTasks接口使用
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameterValue	

修改主机备注信息

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

修改主机备注信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-15 10:32:23。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyMachineRemark
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Quuid	是	否	String	主机Quuid
Remark	否	否	String	备注信息

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

资产指纹启动扫描

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

资产指纹启动扫描

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ScanAsset
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
AssetTypeIds	否	否	Array of Uint64	资产指纹类型id列表
Quuids	否	否	Array of String	Quuid列表

3. 输出参数

参数名称	类型	描述
TaskId	Uint64	任务id
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InternalError.MainDBFail	
FailedOperation.NoProfessionHost	
OperationDenied	

错误码	描述
FailedOperation	

同步资产扫描信息

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

同步资产扫描信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-09-28 15:55:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SyncAssetScan
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Sync	是	否	Bool	是否同步：true-是 false-否；默认false

3. 输出参数

参数名称	类型	描述
LatestEndTime	String	最新结束同步时间
LatestStartTime	String	最新开始同步时间
State	String	枚举值有(大写)：NOTASK（没有同步任务），SYNCING（同步中），FINISHED（同步完成）
TaskId	Uint64	任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InternalError.MainDBFail	
FailedOperation.APIServerFail	
FailedOperation	

关联机器标签列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

关联机器标签列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UpdateMachineTags
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
MachineArea	是	否	String	服务器类型(CVM|BM|ECM|LH|Other)
MachineRegion	是	否	String	服务器地区 如: ap-guangzhou
Quuid	是	否	String	机器 Quuid
TagIds	否	否	Array of Uint64	标签ID，该操作会覆盖原有的标签列表

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

高级防御相关接口
添加网站防护服务器

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

添加网站防护服务器

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateProtectServer
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
ProtectDir	是	否	String	防护目录地址
ProtectHostConfig	是	否	Array of ProtectHostConfig	防护机器 信息

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

删除网络攻击日志

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

删除网络攻击日志

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-10 10:14:54。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteAttackLogs
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	否	否	Array of Uint64	日志ID数组，最大100条。
IsAll	否	否	Bool	是否全部删除

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
LimitExceeded.AreaQuota	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

删除防护网站

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

删除防护网站

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteProtectDir
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of String	删除的目录ID 最大100条

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	
OperationDenied	
InvalidParameterValue	
FailedOperation	

删除事件记录

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

网站防篡改-删除事件记录

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteWebPageEventLog
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of Uint64	**此参数对外不可见。** 需要删除的事件ID 集合 最大100条

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

网络攻击事件详情

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAttackEventInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	Uint64	事件id

3. 输出参数

参数名称	类型	描述
NetAttackEventInfo	NetAttackEventInfo	网络攻击事件详情
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

按分页形式展示网络攻击检测事件列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAttackEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序
Filters	否	否	Array of Filter	过滤条件。
Type - String 攻击状态 0: 尝试攻击 1: 攻击成功 - 是否必填: 否				
Status - String 事件处理状态 0：待处理 1：已处理 2： 已加白 3： 已忽略 4：已删除 - 是否必填: 否				
SrcIP - String 来源IP - 是否必填: 否				
Uuids - String 主机安全uuid - 是否必填: 否				
Quuids - String cvm uuid - 是否必填: 否				
DstPort - String 攻击目标端口 - 是否必填: 否				
MachineName - String 主机名称 - 是否必填: 否				
InstanceID - String 主机实例ID - 是否必填: 否				
AttackTimeBegin - String 攻击开始时间 - 是否必填: 否				
AttackTimeEnd - String 攻击结束时间 - 是否必填: 否				
VulSupportDefense - String 漏洞是否支持防御 0不支持，1支持 - 是否必填: 否				
Limit	否	否	Uint64	返回数量，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	String	排序方式 ASC,DESC

3. 输出参数

参数名称	类型	描述
List	NetAttackEvent	攻击事件列表
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

网络攻击日志详情

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

网络攻击日志详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-10-31 15:59:56。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAttackLogInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	Uint64	日志ID

3. 输出参数

参数名称	类型	描述
CreatedAt	String	攻击时间
DstIp	String	攻击目标IP
DstPort	Uint64	攻击目标端口
HttpCgi	String	攻击路径
HttpContent	String	攻击内容
HttpHead	String	攻击头信息
HttpHost	String	攻击目标主机
HttpMethod	String	攻击方法
HttpParam	String	攻击参数
HttpReferer	String	请求源
HttpUserAgent	String	攻击者浏览器标识
Id	Uint64	日志ID
Quuid	String	主机ID
SrcIp	String	攻击来源IP
SrcPort	Uint64	攻击来源端口
VulType	String	威胁类型
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

网络攻击日志列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

按分页形式展示网络攻击日志列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAttackLogs
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。 - HttpMethod - String - 是否必填：否 - 攻击方法(POST|GET) - DateRange - String - 是否必填：否 - 时间范围(存储最近3个月的数据)，如最近一个月["2019-11-17", "2019-12-17"] - VulType - String 威胁类型 - 是否必填: 否 - SrcIp - String 攻击源IP - 是否必填: 否 - DstIp - String 攻击目标IP - 是否必填: 否 - SrcPort - String 攻击源端口 - 是否必填: 否 - DstPort - String 攻击目标端口 - 是否必填: 否
Limit	否	否	Uint64	返回数量，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。
Quuid	否	否	String	云主机机器ID
Uuid	否	否	String	主机安全客户端ID

3. 输出参数

参数名称	类型	描述
AttackLogs	DefendAttackLog	日志列表
TotalCount	Uint64	总条数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
InvalidParameter	
InvalidParameterValue	

网络攻击数据统计

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAttackStatistics
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AttackSrcIpCount	Uint64	总攻击来源ip数量
AttackedAssetCount	Uint64	总受攻击资产数量
AttackedPortCount	Uint64	总受攻击端口数量
NewAttackSrcIpCount	Uint64	今日新增攻击来源ip数量
NewAttackedAssetCount	Uint64	今日新增受攻击资产数量
NewAttackedPortCount	Uint64	今日新增受攻击端口数量
PendingAttackCount	Uint64	总攻击次数
PendingNewAttackCount	Uint64	今日新增攻击次数
PendingSuccAttackCount	Uint64	总攻击成功次数
PendingTryAttackCount	Uint64	总尝试攻击次数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	

错误码	描述
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

网络攻击top5数据列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAttackTop
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。
BeginTime - String 起始时间,默认近7天- 是否必填: 否				

3. 输出参数

参数名称	类型	描述
NetAttackTopInfo	NetAttackTopInfo	top统计数据
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

网络攻击趋势数据

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAttackTrends
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filter	过滤条件。
BeginTime - String 起始时间,默认近7天- 是否必填: 否				

3. 输出参数

参数名称	类型	描述
NetAttackTrend	NetAttackTrend	攻击趋势统计数据（天）
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

获取网络攻击威胁类型列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

获取网络攻击威胁类型列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAttackVulTypeList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
List	String	威胁类型列表
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

网页防篡改获取区域主机列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

用于网页防篡改获取区域主机列表。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMachineList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of AssetFilters	过滤条件。 - Keywords - String - 是否必填：否 - 查询关键字 - Status - String - 是否必填：否 - 客户端在线状态（OFFLINE: 离线 | ONLINE: 在线 | UNINSTALLED：未安装） - Version - String 是否必填：否 - 当前防护版本（ PRO_VERSION：专业版 | BASIC_VERSION：基础版） 每个过滤条件只支持一个值，暂不支持多个值"或"关系查询
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。
MachineRegion	是	否	String	机器所属地域。如：ap-guangzhou，ap-shanghai
MachineType	是	否	String	云主机类型。 - CVM：表示虚拟主机 - BM: 表示黑石物理机 - ECM: 表示边缘计算服务器 - LH: 表示轻量应用服务器 - Other: 表示混合云机器
Offset	否	否	Uint64	偏移量，默认为0。

3. 输出参数

参数名称	类型	描述
Machines	Machine	主机列表
TotalCount	Uint64	主机数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	

错误码	描述
InvalidParameter.InvalidFormat	
MissingParameter	
FailedOperation.APIServerFail	
InvalidParameter	
InvalidParameterValue	

查询网络攻击设置

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeNetAttackSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
MemberId	否	否	Array of String	集团账号的成员id

3. 输出参数

参数名称	类型	描述
AutoInclude	Uint64	新增资产自动包含 0 不包含 1包含
ExcludeInstanceIds	String	自选排除主机
InstanceIds	String	自选主机
NetAttackAlarmStatus	Uint64	0 新增告警事件默认待处理，1新增告警事件默认已处理，3新增告警事件默认忽略
NetAttackEnable	Uint64	0 关闭网络攻击检测，1开启网络攻击检测
Scope	Uint64	1 全部旗舰版主机，0 InstanceIds列表主机
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	

错误码	描述
InvalidParameterValue	

防护目录列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

网页防篡改防护目录列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeProtectDirList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序字段
Filters	否	否	Array of AssetFilters	DirName 网站名称 DirPath 网站防护目录地址
Limit	是	否	Uint64	分页条数 最大100条
Offset	是	否	Uint64	偏移量
Order	否	否	String	asc：升序/desc：降序

3. 输出参数

参数名称	类型	描述
List	ProtectDirInfo	防护目录列表信息
TotalCount	Uint64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

查询防护目录关联服务器

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询防护目录关联服务器列表信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeProtectDirRelatedServer
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序值
Filters	否	否	Array of Filter	过滤参数 ProtectStatus
Id	是	否	String	唯一ID
Limit	是	否	Uint64	分页条数 最大100条
Offset	是	否	Uint64	偏移量
Order	否	否	String	排序方式

3. 输出参数

参数名称	类型	描述
List	ProtectDirRelatedServer	网站关联服务器列表信息
ProtectServerCount	Uint64	已开启防护总数
TotalCount	Uint64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	

错误码	描述
InvalidParameterValue	

查询服务器关联目录详情

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询服务区关联目录详情

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeServerRelatedDirInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	Uint64	唯一ID

3. 输出参数

参数名称	类型	描述
HostIp	String	服务器IP
HostName	String	服务器名称
ProtectDirNum	Uint64	防护目录数量
ProtectFileNum	Uint64	防护文件数量
ProtectLinkNum	Uint64	防护软链数量
ProtectTamperNum	Uint64	防篡改数量
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

查询篡改事件列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询篡改事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeWebPageEventList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序方式：CreateTime 或 RestoreTime，默认为CreateTime
Filters	否	否	Array of AssetFilters	过滤条件 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - EventType - String - 是否必填：否 - 事件类型 - EventStatus - String - 是否必填：否 - 事件状态
Limit	否	否	Uint64	返回数量，默认为10，最大值为100。
Offset	否	否	Uint64	偏移量，默认为0。
Order	否	否	Uint64	排序方式，0降序，1升序，默认为0

3. 输出参数

参数名称	类型	描述
List	ProtectEventLists	防护事件列表信息
TotalCount	Uint64	总数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

查询网页防篡改概览信息

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

查询网站防篡改概览信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeWebPageGeneralize
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
ProtectDirNum	Uint64	防护目录数
ProtectFileNum	Uint64	防护文件数
ProtectHostNum	Uint64	防护主机数
ProtectMonitor	Uint64	防护监测 0 未开启 1 已开启 2 异常
ProtectToday	Uint64	今日防护数
TamperFileNum	Uint64	篡改文件数
TamperNum	Uint64	篡改数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

查询网页防篡改防护统计

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

网站防篡改-查询动态防护信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeWebPageProtectStat
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
FileTamperNum	ProtectStat	文件篡改信息
ProtectFileType	ProtectStat	防护文件分类信息
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

查询网站防篡改服务信息

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

网站防篡改-查询网页防篡改服务器购买信息及服务器信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeWebPageServiceInfo
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
AllAuthorizedMachines	ProtectMachineInfo	所有授权机器信息
BuyNum	Uint64	已购授权数
ExpireAuthorizedMachines	ProtectMachine	临近到期授权机器信息
ExpireNum	Uint64	临近到期数量
ExpiredNum	Uint64	已过期授权数
ProtectDirNum	Uint64	防护目录数
ResidueNum	Uint64	剩余授权数
Status	Bool	是否已购服务：true-是，false-否
UsedNum	Uint64	已使用授权数
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	

导出网络攻击事件

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportAttackEvents
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序值 CreateTime
Filters	否	否	Array of Filters	过滤参数。 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - FilePath - String - 是否必填：否 - 路径筛选 - VirusName - String - 是否必填：否 - 描述筛选 - CreateBeginTime - String - 是否必填：否 - 创建时间筛选-开始时间 - CreateEndTime - String - 是否必填：否 - 创建时间筛选-结束时间 - Status - String - 是否必填：否 - 状态筛选
Order	否	否	String	排序 方式 ，ASC，DESC

3. 输出参数

参数名称	类型	描述
TaskId	String	任务ID,需要到接口"异步导出任务"ExportTasks获取DownloadUrl下载地址
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	
InvalidParameterValue	

导出网络攻击日志

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出网络攻击日志

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:34。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportAttackLogs
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Filters	否	否	Array of Filters	过滤条件。 - HttpMethod - String - 是否必填：否 - 攻击方法(POST|GET) - DateRange - String - 是否必填：否 - 时间范围(存储最近3个月的数据)，如最近一个月["2019-11-17", "2019-12-17"] - VulType - String 威胁类型 - 是否必填: 否 - SrcIp - String 攻击源IP - 是否必填: 否 - DstIp - String 攻击目标IP - 是否必填: 否 - SrcPort - String 攻击源端口 - 是否必填: 否 - DstPort - String 攻击目标端口 - 是否必填: 否
Quuid	否	否	String	云主机机器ID
Uuid	否	否	String	主机安全客户端ID

3. 输出参数

参数名称	类型	描述
DownloadUrl	String	已废弃
TaskId	String	导出任务ID 可通过ExportTasks接口下载
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
FailedOperation.Export	
InvalidParameter	

错误码	描述
InvalidParameterValue	

导出防护目录列表

最近更新时间: 2024-09-03 18:50:08

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出网页防篡改防护目录列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportProtectDirList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序字段
Filters	否	否	Array of AssetFilters	DirName 网站名称 DirPath 网站防护目录地址
Order	否	否	String	asc：升序/desc：降序

3. 输出参数

参数名称	类型	描述
TaskId	String	任务ID
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
InvalidParameter	
InvalidParameterValue	

导出篡改事件列表

最近更新时间: 2024-09-03 18:50:09

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

导出篡改事件列表

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ExportWebPageEventList
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
By	否	否	String	排序方式：CreateTime 或 RestoreTime，默认为CreateTime
Filters	否	否	Array of AssetFilters	过滤条件 - IpOrAlias - String - 是否必填：否 - 主机ip或别名筛选 - EventType - String - 是否必填：否 - 事件类型 - EventStatus - String - 是否必填：否 - 事件状态
Order	否	否	Uint64	排序方式，0降序，1升序，默认为0

3. 输出参数

参数名称	类型	描述
TaskId	String	任务id 可通过 ExportTasks接口下载
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.MissingParameter	
MissingParameter	
InvalidParameter	
InvalidParameterValue	

修改网络攻击设置

最近更新时间: 2024-09-03 18:50:09

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

yunapi response

默认接口请求频率限制：20次/秒。

接口更新时间：0001-01-01 00:00:00。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyNetAttackSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
AutoInclude	否	否	Uint64	新增资产自动包含 0 不包含 1包含
ExcludeInstanceIds	否	否	Array of String	自选排除的主机
InstanceIds	否	否	Array of String	自选主机
MemberId	否	否	Array of String	集团账号的成员id
NetAttackAlarmStatus	是	否	Uint64	0 新增告警事件默认待处理，1新增告警事件默认已处理，3新增告警事件默认忽略
NetAttackEnable	是	否	Uint64	0 关闭网络攻击检测，1开启网络攻击检测
Scope	否	否	Uint64	1 全部旗舰版主机，0 Quuids列表主机

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
MissingParameter	
ResourceNotFound	
InvalidParameter	
OperationDenied	

错误码	描述
InvalidParameterValue	

创建网站防护目录

最近更新时间: 2024-09-03 18:50:09

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

创建/修改网站防护目录

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:12:33。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyWebPageProtectDir
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
HostConfig	是	否	Array of ProtectHostConfig	防护机器列表信息
ProtectDirAddr	是	否	String	网站防护目录地址
ProtectDirName	是	否	String	网站防护目录名称
ProtectFileType	是	否	String	防护文件类型,分号分割；

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.MissingParameter	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter.IllegalRequest	
FailedOperation.AgentOffline	
FailedOperation.APIServerFail	
FailedOperation.LicenseExceeded	
InvalidParameter	
OperationDenied	

错误码	描述
InvalidParameterValue	
FailedOperation	
FailedOperation.ProtectStartFail	

修改网站防护设置

最近更新时间: 2024-09-03 18:50:09

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

修改网站防护设置

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyWebPageProtectSetting
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Id	是	否	String	配置对应的protect_path
ModifyType	是	否	Uint64	需要操作的类型1 目录名称 2 防护文件类型
Value	是	否	String	提交值

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.ParsingError	
InvalidParameter.InvalidFormat	
MissingParameter	
InvalidParameter	
InvalidParameterValue	
FailedOperation	

网站防护设置开关

最近更新时间: 2024-09-03 18:50:09

1. 接口描述

接口请求域名： cwp.api3.cloud.sunhongs.com。

网站防篡改防护设置开关

默认接口请求频率限制：20次/秒。

接口更新时间：2022-05-20 15:13:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyWebPageProtectSwitch
Version	是	否	String	公共参数，本接口取值：2018-02-28
Region	是	否	String	公共参数，本接口不需要传递此参数。
Ids	是	否	Array of String	需要操作开关的网站 最大100条
Status	否	否	Uint64	1 开启 0 关闭 SwitchType 为 1 | 2 必填;
SwitchType	是	否	Uint64	开关类型 1 防护开关 2 自动恢复开关 3 移除防护目录

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	
InvalidParameter.InvalidFormat	
MissingParameter	
ResourceNotFound	
FailedOperation.AgentOffline	
FailedOperation.APIServerFail	
FailedOperation.LicenseExceeded	
InvalidParameter	
LimitExceeded	

错误码	描述
OperationDenied	
FailedOperation	

数据结构

最近更新时间: 2024-09-03 18:50:09

Process

进程信息数据。

被如下接口引用：DescribeProcesses

名称	必选	允许NULL	类型	描述
CreateTime	是	否	Datetime	创建时间。
FullPath	是	否	String	进程路径。
Id	是	否	Uint64	唯一ID。
MachineIp	是	否	String	主机内网IP。
MachineName	是	否	String	主机名。
Pid	是	否	Uint64	进程Pid。
Platform	是	否	String	所属平台。 - WIN32：windows32位 - WIN64：windows64位 - LINUX32：Linux32位 - LINUX64：Linux64位
Ppid	是	否	Uint64	进程Ppid。
ProcessName	是	否	String	进程名。
Username	是	否	String	进程用户名。
Uuid	是	否	String	云镜客户端唯一UUID。

AssetWebLocationPath

资产管理Web站点虚拟目录

被如下接口引用：DescribeAssetWebLocationPathList

名称	必选	允许NULL	类型	描述
Group	是	否	String	文件所属组
Permission	是	否	String	文件权限
RealPath	是	否	String	物理路径
User	是	否	String	文件所有者
VirtualPath	是	否	String	虚拟路径

MachineExtraInfo

服务器基础信息

被如下接口引用：DescribeAssetAppList、DescribeAssetCoreModuleList、DescribeAssetDatabaseList、DescribeAssetEnvList、DescribeAssetInitServiceList、DescribeAssetJarList、DescribeAssetMachineDetail、DescribeAssetMachineList、DescribeAssetPlanTaskList、DescribeAssetPortInfoList、DescribeAssetProcessInfoList、DescribeAssetUserList、DescribeAssetWebAppList、DescribeAssetWebFrameJarList、DescribeAssetWebFrameList、DescribeAssetWebLocationList、DescribeAssetWebServiceInfoList、DescribeAttackEventInfo、DescribeAttackEvents、DescribeAttackLogs、DescribeBaselineFixList、DescribeBaselineHostDetectList、DescribeBaselineHostIgnoreList、DescribeBaselineItemList、DescribeBashEventsNew、DescribeBruteAttackList、DescribeDefenceEventDetail、DescribeFileTamperEvents、DescribeHostLoginList、DescribeIgnoreHostAndItemConfig、DescribeJavaMemShellInfo、DescribeJavaMemShellList、DescribeJavaMemShellPluginList、DescribeLicenseBindList、DescribeMachineList、DescribeMachines、DescribeMalWareList、DescribeMalwareInfo、DescribePrivilegeEvents、DescribeProtectDirRelatedServer、DescribeReverseShellEvents、DescribeRiskDnsEventInfo、DescribeRiskDnsEventList、DescribeRiskProcessEvents、DescribeScanTaskDetails、DescribeScreenMachines、DescribeVulDefenceEvent、DescribeVulEffectHostList、DescribeWebPageEventList

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
HostName	否	是	String	主机名
InstanceID	否	是	String	实例ID
NetworkName	否	是	String	网络名，vpc网络情况下会返回vpc_id
NetworkType	否	是	Int64	网络类型，1:vpc网络 2:基础网络 3:非腾讯云网络
PrivateIP	否	是	String	内网IP
WanIP	否	是	String	公网IP

SecurityDynamic

安全事件消息数据。

被如下接口引用：DescribeSecurityDynamics

名称	必选	允许NULL	类型	描述
EventTime	是	否	Datetime	安全事件发生时间。
EventType	是	否	String	安全事件类型。 - MALWARE：木马事件 - NON_LOCAL_LOGIN：异地登录 - BRUTEATTACK_SUCCESS：密码破解成功 - VUL：漏洞 - BASELINE：安全基线
Message	是	否	String	安全事件消息。
SecurityLevel	是	否	String	安全事件等级。
RISK: 严重				
HIGH: 高危				
NORMAL: 中危				
LOW: 低危				
UNKNOWNED: 可疑				
Uuid	是	否	String	云镜客户端UUID。

AssetWebAppBaseInfo

资源管理Web应用列表信息

被如下接口引用：DescribeAssetWebAppList

名称	必选	允许NULL	类型	描述
Desc	否	否	String	应用描述
Domain	否	否	String	站点域名
FirstTime	否	否	String	首次采集时间
Id	否	否	String	应用ID
IsNew	否	否	Int64	是否新增[0:否|1:是]
MachineExtraInfo	否	是	MachineExtraInfo	附加信息

名称	必选	允许NULL	类型	描述
MachineIp	否	否	String	主机内网IP
MachineName	否	否	String	主机名称
MachineWanIp	否	否	String	主机外网IP
Name	否	否	String	应用名
OsInfo	否	否	String	操作系统信息
PluginCount	否	否	Uint64	插件数
ProjectId	否	否	Uint64	主机业务组ID
Quuid	否	否	String	主机Quuid
RootPath	否	否	String	根路径
ServiceType	否	否	String	服务类型
Tag	否	是	Array of MachineTag	主机标签
UpdateTime	否	是	String	数据更新时间
Uuid	否	否	String	主机Uuid
Version	否	否	String	版本
VirtualPath	否	否	String	虚拟路径

Tags

平台标签

被如下接口引用：CreateLicenseOrder、DescribeHostInfo、DescribeImportMachineInfo、DescribeLicenseList、DescribeMachineList、DescribeMachines、DescribeMachinesSimple、DescribeVulEffectHostList、ExportLicenseDetail

名称	必选	允许NULL	类型	描述
TagKey	是	否	String	标签键
TagValue	是	否	String	标签值

Data

断电演习 - 业务恢复检测接口： Mol为分子，Den为分母，表示业务的恢复量化指标，最终呈现结果即为“（ Mol/Den ）*100%”计算后的百分比，例如 Mol为3，Den为10，则结果为30%，表示请求接口的这个时间点业务恢复30%

被如下接口引用：

名称	必选	允许NULL	类型	描述
Den	是	否	Uint64	分母
Mol	是	否	Uint64	分子
Time	是	是	String	时间，如果不返回，将使用请求当前时间

BaselinePassword

基线密码

被如下接口引用：

名称	必选	允许NULL	类型	描述
Password	是	否	String	密码
Username	是	否	String	用户名

MalwareWhiteListAffectEvent

木马白名单影响事件信息

被如下接口引用：DescribeMalwareWhiteListAffectList

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	添加时间
FilePath	是	否	String	文件路径
HostIp	是	否	String	主机ip
Id	是	否	Uint64	唯一ID。
Md5	是	否	String	影响的md5

ScreenRegionInfo

地域信息

被如下接口引用：DescribeScreenMachineRegions

名称	必选	允许NULL	类型	描述
Region	是	否	String	地域标志，如 ap-guangzhou，ap-shanghai，ap-beijing
RegionCode	是	否	String	地域代码，如 gz，sh，bj
RegionId	是	否	Uint64	地域ID
RegionName	是	否	String	地域中文名，如华南地区（广州），华东地区（上海金融），华北地区（北京）
RegionNameEn	是	否	String	地域英文名

AttackSourceEvent

攻击溯源事件

被如下接口引用：DescribeAttackSourceEvents

名称	必选	允许NULL	类型	描述
Content	是	否	String	【文件查杀】病毒名 VirusName、文件名 FileName、文件路径 FilePath、文件大小 FileSize、文件MD5 MD5、首次发现时间 CreateTime、最近检测时间LatestScanTime、危害描述 HarmDescribe、修复建议 SuggestScheme【异常登录】来源IP SrcIp、来源地 Location、登录用户名 UserName、登录时间 LoginTime【密码破解】来源IP SrcIp、来源地 City,Country 、协议 Protocol、登录用户名UserName 、端口 Port、尝试次数 Count、首次攻击时间 CreateTime、最近攻击时间 ModifyTime【恶意请求】恶意请求域名 Url、进程ProcessName 、MD5 ProcessMd5、PID Pid、请求次数 AccessCount、最近请求时间 MergeTime、危害描述 HarmDescribe、修复建议SuggestScheme【高危命令】命中规则名 RuleName、规则类别 RuleCategory、命令内容 BashCmd、数据来源 DetectBy、登录用户 User、PID Pid、发生时间 CreateTime 、危害描述 HarmDescribe、修复建议SuggestScheme
CreatedTime	是	否	String	入侵时间
EventType	是	否	Uint64	事件类型：0：文件查杀，1：异常登录， 2：密码破解，3：恶意请求，4：高危命令
Id	是	否	Uint64	事件id

名称	必选	允许NULL	类型	描述
Level	是	否	Uint64	等级 事件统一等级 0：提示，1：低危, 2：中危, 3：高危, 4：严重
LevelZh	是	否	String	等级中文展示字符串
Uuid	是	否	String	主机uuid

ProtectMachineInfo

授权机器信息

被如下接口引用：DescribeWebPageServiceInfo

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	开通时间
ExpireTime	是	否	String	到期时间
HostIp	是	否	String	机器IP
HostName	是	否	String	机器名称

MiniSite

站点信息。

被如下接口引用：

名称	必选	允许NULL	类型	描述
SiteId	是	否	Uint64	站点ID。
Url	是	否	String	站点Url。

HostDesc

展示登录审计白名单时的主机信息实体

被如下接口引用：DescribeLoginWhiteHostList

名称	必选	允许NULL	类型	描述
MachineIp	是	否	String	机器IP:已销毁的服务器IP为空
MachineName	是	否	String	机器名
MachineWanIp	是	否	String	公网IP:已销毁的服务器IP为空
Quuid	是	否	String	云镜客户端ID
Tags	是	否	Array of MachineTag	标签信息数组
Uuid	是	否	String	主机ID

ScreenAttackHotspot

大屏全网攻击热点

被如下接口引用：DescribeScreenAttackHotspot

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
CreatedTime	是	否	String	时间
DstIp	是	否	String	受害者IP
EventName	是	否	String	事件名
Region	是	否	String	地域
SrcIp	是	否	String	攻击者IP

DeliverTypeDetails

日志投递类型细节

被如下接口引用：DescribeLogKafkaDeliverInfo、ModifyLogKafkaAccess

名称	必选	允许NULL	类型	描述
ErrInfo	否	否	String	错误信息
LogType	是	否	Array of Int64	安全模块下的日志类型， http://tapd.woa.com/Teneyes/markdown_wikis/show/#1210131751002328905
SecurityType	是	否	Uint64	安全模块类型 1: 入侵检测 2: 漏洞管理 3: 基线管理 4: 高级防御 5:客户端相关 6: 资产指纹
Status	否	否	Uint64	投递状态，0未开启 1正常 2异常
StatusTime	否	否	Int64	最近一次状态上报时间戳，s
Switch	是	否	Uint64	投递开关 0关闭 1开启
TopicId	是	否	String	kafka topic id
TopicName	是	否	String	kafka topic name

AssetDatabaseDetail

资源管理数据库列表信息

被如下接口引用：DescribeAssetDatabaseInfo

名称	必选	允许NULL	类型	描述
BinPath	是	否	String	二进制路径
ConfigPath	是	否	String	配置文件路径
DataPath	是	否	String	数据路径
ErrorLogPath	是	否	String	错误日志路径
Ip	是	否	String	绑定IP
LogPath	是	否	String	日志文件路径
MachineIp	是	否	String	主机内网IP
MachineWanIp	是	否	String	主机外网IP
Name	是	否	String	数据库名
OsInfo	是	否	String	操作系统信息
Param	是	否	String	启动参数
Permission	是	否	String	运行权限

名称	必选	允许NULL	类型	描述
PlugInPath	是	否	String	插件路径
Port	是	否	String	监听端口
Proto	是	否	String	协议
Quuid	是	否	String	主机Quuid
UpdateTime	是	是	String	数据更新时间
User	是	否	String	运行用户
Uuid	是	否	String	主机Uuid
Version	是	否	String	版本

JavaMemShellPluginInfo

Java内存马插件信息

被如下接口引用：DescribeJavaMemShellPluginInfo

名称	必选	允许NULL	类型	描述
ErrorLog	是	否	String	错误日志
MainClass	是	否	String	注入进程主类
Pid	是	否	Uint64	注入进程pid
Status	是	否	Uint64	注入状态：0: 注入中, 1: 注入成功, 2: 插件超时, 3: 插件退出, 4: 注入失败 5: 软删除

BaselineCustomRuleIdName

基线自定规则ID和名字

被如下接口引用：DescribeBaselineItemIgnoreList、DescribeBaselineItemInfo、DescribeIgnoreHostAndItemConfig

名称	必选	允许NULL	类型	描述
RuleId	是	是	Int64	自定义规则ID
RuleName	是	是	String	自定义规则名字

BruteAttack

暴力破解列表

被如下接口引用：DescribeBruteAttacks

名称	必选	允许NULL	类型	描述
BanStatus	是	否	String	阻断状态。
City	是	否	Uint64	城市ID。
Count	是	否	Uint64	尝试破解次数。
Country	是	否	Uint64	国家ID。
CreateTime	是	否	Datetime	发生时间。
Id	是	否	Uint64	事件ID。

名称	必选	允许NULL	类型	描述
IsProVersion	是	否	Bool	是否专业版。
MachineIp	是	否	String	主机IP。
MachineName	是	否	String	主机名称。
Province	是	否	Uint64	省份ID。
Quuid	是	否	String	机器UUID
SrcIp	是	否	String	来源IP。
Status	是	否	String	破解事件状态 - BRUTEATTACK_FAIL_ACCOUNT： 暴力破解事件-失败(存在帐号) - BRUTEATTACK_FAIL_NOACCOUNT：暴力破解事件-失败(帐号不存在) - BRUTEATTACK_SUCCESS：暴力破解事件-成功
UserName	是	否	String	用户名称。
Uuid	是	否	String	云镜客户端唯一标识UUID。

MaliciousRequestWhiteListInfo

恶意请求白名单列表信息

被如下接口引用：DescribeMaliciousRequestWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建时间
Domain	是	否	String	域名
Id	是	否	Uint64	白名单id
Mark	是	否	String	备注
ModifyTime	是	否	String	更新时间

WeeklyReportNonlocalLoginPlace

专业周报异地登录数据。

被如下接口引用：DescribeWeeklyReportNonlocalLoginPlaces

名称	必选	允许NULL	类型	描述
City	是	否	Uint64	城市ID。
Country	是	否	Uint64	国家ID。
LoginTime	是	否	Datetime	登录时间。
MachineIp	是	否	String	主机IP。
Province	是	否	Uint64	省份ID。
SrcIp	是	否	String	源IP。
Username	是	否	String	用户名。

AssetProcessBaseInfo

资源管理进程基本信息

被如下接口引用：DescribeAssetProcessInfoList

名称	必选	允许NULL	类型	描述
Desc	否	否	String	进程说明
FirstTime	否	否	String	首次采集时间
GroupName	否	否	String	进程用户组
HasSign	否	否	Uint64	数字签名:0无，1有， 999 空，仅windows
InstallByPackage	否	否	Uint64	是否通过安装包安装：:0否，1是， 999 空，仅linux
IsNew	否	否	Int64	是否新增[0:否|1:是]
MachineExtraInfo	否	是	MachineExtraInfo	
附加信息				
MachineIp	否	否	String	主机内网IP
MachineName	否	否	String	主机名称
MachineWanIp	否	否	String	主机外网IP
Md5	否	否	String	进程MD5
Name	否	否	String	进程名称
OsInfo	否	否	String	操作系统信息
PackageName	否	否	String	软件包名
Param	否	否	String	启动参数
ParentProcessName	否	否	String	父进程名称
Path	否	否	String	进程路径
Pid	否	否	String	进程ID
Ppid	否	否	String	父进程ID
ProjectId	否	否	Uint64	主机业务组ID
Quuid	否	否	String	主机Quuid
StartTime	否	否	String	启动时间
Status	否	否	String	进程状态
Tag	否	是	Array of MachineTag	主机标签
Tty	否	否	String	进程TTY
UpdateTime	否	是	String	数据更新时间
User	否	否	String	运行用户
Uuid	否	否	String	主机Uuid
Version	否	否	String	进程版本

VulFixStatusInfo

查看漏洞修复详情

被如下接口引用：DescribeVulFixStatus

名称	必选	允许NULL	类型	描述
FailCnt	是	是	Uint64	漏洞修复失败主机数量

名称	必选	允许NULL	类型	描述
FixSuccessCnt	是	是	Uint64	修复成功的数量
HostList	是	是	Array of VulFixStatusHostInfo	漏洞对应主机修复状态
Progress	是	否	Uint64	漏洞修复进度 1-100；
VulId	是	是	Uint64	漏洞id
VulName	是	是	String	漏洞名称

AlarmSettings

告警设置

被如下接口引用：

名称	必选	允许NULL	类型	描述
DisableMailWarning	是	否	String	邮件告警。
DisablePhoneWarning	是	否	String	手机告警。
DisableWebWarning	是	否	String	网页告警。

CKafkaRouteInfo

CKafka域名信息

被如下接口引用：DescribeLogDeliveryKafkaOptions

名称	必选	允许NULL	类型	描述
AccessType	是	否	Int64	接入类型
Domain	是	否	String	域名
DomainPort	是	否	Uint64	域名端口
RouteID	是	否	Int64	路由ID
Vip	是	否	String	虚拟ip
VipType	是	否	Int64	虚拟ip类型

ConfigUUIDInfo

主机安全-新增文件防护

被如下接口引用：

名称	必选	允许NULL	类型	描述
ConfigId	是	是	Uint64	文件防护ID
UUID	是	是	String	服务器ID

VulEmergentMsgInfo

紧急通知实体

被如下接口引用：DescribeVulEmergentMsg

名称	必选	允许NULL	类型	描述
Name	是	否	String	漏洞名
PublishTime	是	否	String	漏洞纰漏时间
VulId	是	否	Uint64	漏洞id

VulInfoByCveId

根据cve_id查询漏洞详情

被如下接口引用：DescribeVulCveIdInfo

名称	必选	允许NULL	类型	描述
FixSwitch	是	否	Uint64	修复支持情况：0-windows/linux均不支持修复 ;1-windows/linux 均支持修复 ;2-仅linux支持修复;3-仅windows支持修复
VulId	是	否	Uint64	漏洞id

City

城市信息

被如下接口引用：

名称	必选	允许NULL	类型	描述
CityId	是	否	String	城市Id
ProvinceId	是	否	String	省份Id

AssetWebAppPluginInfo

资产管理Web应用插件详情

被如下接口引用：DescribeAssetWebAppPluginList

名称	必选	允许NULL	类型	描述
Desc	是	否	String	描述
Link	是	否	String	链接
Name	是	否	String	名称
Version	是	否	String	版本

BashEventsInfo

高危命令数据详情

被如下接口引用：DescribeBashEventsInfo

名称	必选	允许NULL	类型	描述
BashCmd	是	否	String	执行命令
CreateTime	是	否	String	发生时间
DetectBy	否	是	Int64	检测来源 0:bash日志 1:实时监控
Exe	是	是	String	进程名称

名称	必选	允许NULL	类型	描述
HarmDescribe	是	是	String	描述
HostIp	是	否	String	主机内网IP
Id	是	否	Uint64	数据ID
MachineName	是	否	String	主机名
MachineStatus	是	是	String	主机在线状态 OFFLINE ONLINE
MachineWanIp	是	是	String	主机外网ip
ModifyTime	是	是	String	处理时间
Pid	是	是	String	进程号
Platform	是	否	Uint64	平台类型
PsTree	是	是	String	进程树 json pid:进程id，exe:文件路径 ，account:进程所属用组和用户 ,cmdline:执行命令，ssh_service:SSH服务ip, ssh_soure:登录源
Quuid	是	否	String	主机ID
References	是	是	Array of String	参考链接
RegexBashCmd	是	是	String	自动生成的正则表达式
RuleCategory	是	是	Uint64	规则类别 0=系统规则，1=用户规则
RuleId	是	否	Uint64	规则ID,等于0表示已规则已被删除或生效范围已修改
RuleLevel	是	否	Uint64	规则等级：1-高 2-中 3-低
RuleName	是	否	String	规则名称
Status	是	否	Uint64	处理状态： 0 = 待处理 1= 已处理, 2 = 已加白， 3= 已忽略
SuggestScheme	是	是	String	建议方案
Tags	是	是	Array of String	标签
User	是	是	String	登录用户
Uuid	是	否	String	云镜ID

UsualPlace

常用登录地

被如下接口引用：DescribeUsualLoginPlaces

名称	必选	允许NULL	类型	描述
CityId	是	否	Uint64	城市 ID。
CountryId	是	否	Uint64	国家 ID。
Id	是	否	Uint64	ID。
ProvinceId	是	否	Uint64	省份 ID。
Uuid	是	否	String	云镜客户端唯一标识UUID。

ScreenEmergentMsg

大屏可视化紧急通知

被如下接口引用：DescribeScreenEmergentMsg

名称	必选	允许NULL	类型	描述
Text	是	否	String	通知内容
Title	是	否	String	通知标签/标题
Type	是	否	Uint64	跳转类型：0=漏洞管理

BaselineBasicInfo

基线基础信息

被如下接口引用：DescribeBaselineBasicInfo

名称	必选	允许NULL	类型	描述
BaselineId	是	是	Uint64	基线id
Name	是	是	String	基线名称
ParentId	是	是	Uint64	父级id

VulHostTopInfo

服务器风险top5实体

被如下接口引用：DescribeVulHostTop

名称	必选	允许NULL	类型	描述
HostName	是	是	String	主机名
Quuid	是	是	String	主机Quuid
Score	是	是	Uint64	top评分
VulLevelList	是	是	Array of VulLevelCountInfo	漏洞等级与数量统计列表

DefendAttackLog

网络攻击日志

被如下接口引用：DescribeAttackLogs

名称	必选	允许NULL	类型	描述
CreatedAt	否	否	String	攻击时间
DstIp	否	否	String	目标IP
DstPort	否	否	Uint64	目标端口
HttpCgi	否	否	String	攻击描述
HttpContent	否	否	String	攻击内容
HttpMethod	否	否	String	攻击方式
HttpParam	否	否	String	攻击参数
Id	否	否	Uint64	日志ID
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息

名称	必选	允许NULL	类型	描述
MachineIp	否	否	String	目标服务器IP
MachineName	否	否	String	目标服务器名称
SrcIp	否	否	String	来源IP
SrcPort	否	否	Uint64	来源端口
Uuid	否	否	String	客户端ID
VulType	否	否	String	威胁类型

ScreenProtectionCnt

大屏可视化主机安全返回态势数据

被如下接口引用：DescribeScreenProtectionCnt

名称	必选	允许NULL	类型	描述
Count	是	否	Uint64	总数
Name	是	否	String	cloud：云查杀引擎，detect：检测引擎，defend：攻击防御，threat：威胁情报，analysis：异常分析，ai：AI引擎
Type	是	否	String	cloud：云查杀引擎，detect：检测引擎，defend：攻击防御，threat：威胁情报，analysis：异常分析，ai：AI引擎

SecurityButlerInfo

安全管家列表信息

被如下接口引用：DescribeExpertServiceList

名称	必选	允许NULL	类型	描述
EndTime	是	否	String	服务结束时间
HostIp	是	否	String	主机Ip
HostName	是	否	String	主机名称
Id	是	否	Uint64	数据id
OrderId	是	否	Uint64	订单id
Quuid	是	否	String	cvm id
RiskCount	是	否	Uint64	主机风险数
StartTime	是	否	String	服务开始时间
Status	是	否	Uint64	服务状态 0-服务中,1-已到期 2已销毁
Uuid	是	否	String	主机 uuid

ProtectHostConfig

防护机器信息

被如下接口引用：CreateProtectServer、ModifyWebPageProtectDir

名称	必选	允许NULL	类型	描述
AutoRecovery	是	否	Uint64	自动恢复开关 0 关闭 1开启

名称	必选	允许NULL	类型	描述
ProtectSwitch	是	否	Uint64	防护开关 0 关闭 1开启
Quuid	是	否	String	机器唯一ID

RegionSet

地域信息

被如下接口引用：DescribeBanRegions

名称	必选	允许NULL	类型	描述
RegionName	是	否	String	地域名称
ZoneSet	是	否	Array of ZoneInfo	可用区信息

BaselineFix

基线密码修复

被如下接口引用：DescribeBaselineFixList

名称	必选	允许NULL	类型	描述
CreateTime	否	否	String	首次检测时间
FixTime	否	否	String	修复时间
HostIp	否	否	String	主机Ip
Id	否	否	Int64	基线检测项结果ID
ItemName	否	否	String	修复项名称
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
ModifyTime	否	否	String	最后检测时间

ImageHost

容器安全 主机镜像关联列表

被如下接口引用：

名称	必选	允许NULL	类型	描述
HostID	是	否	String	主机id
ImageID	是	否	String	镜像id

AssetLoadDetail

资产管理负载信息

被如下接口引用：DescribeAssetLoadInfo

名称	必选	允许NULL	类型	描述
Desc	是	否	String	描述
MachineName	是	否	String	主机名称

名称	必选	允许NULL	类型	描述
Quuid	是	否	String	主机Quuid
Uuid	是	否	String	主机Uuid
Value	是	否	Float	负载

VulDefenceOverview

漏洞防御趋势页，包括插件状态及攻防趋势，趋势由三个长度相同，元素一一对应的数组保存，如果某天没有数据将会缺失

被如下接口引用：DescribeVulDefenceOverview

名称	必选	允许NULL	类型	描述
AttackCounts	是	是	Array of Int64	每日攻击趋势
Date	是	是	Array of String	日期
DefendCounts	是	是	Array of Int64	每日防御趋势
DefendHostCount	是	否	Int64	已开启防御主机数
Enable	是	否	Int64	防御开关：0 关闭 1 开启
ExceptionCount	是	否	Int64	插件异常数

ScreenBroadcasts

大屏可视化安全播报内容

被如下接口引用：DescribeScreenBroadcasts

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	文章ID
Level	是	否	Uint64	播报文章危险程度 0：无， 1：严重， 2: 高危， 3:中危， 4: 低危
Time	是	否	String	发布时间
Title	是	否	String	播报文章标题

ComponentStatistics

组件统计数据。

被如下接口引用：DescribeComponentStatistics

名称	必选	允许NULL	类型	描述
ComponentName	是	否	String	组件名称。
ComponentType	是	否	String	组件类型。 - WEB：Web组件 - SYSTEM：系统组件
Description	是	否	String	组件描述。
Id	是	否	Uint64	组件ID。
MachineNum	是	否	Uint64	主机数量。

DefaultStrategyInfo

默认策略基础信息

被如下接口引用：DescribeBaselineDefaultStrategyList

名称	必选	允许NULL	类型	描述
StrategyId	是	否	Uint64	策略id
StrategyName	是	否	String	策略名

VulEventList

漏洞动态列表对象

被如下接口引用：DescribeEventList

名称	必选	允许NULL	类型	描述
AliasName	是	否	String	主机别名
Descript	是	否	String	漏洞描述
HostIp	是	否	String	HostIp
Id	是	否	Uint64	漏洞事件id
IfProfession	是	否	Bool	是否为专业版防护
LastTime	是	否	String	最后检测时间
Level	是	否	Uint64	漏洞等级 1:低 2:中 3:高 4:提示
Name	是	否	String	漏洞名称
PublishTime	是	否	String	漏洞披露时间
Quuid	是	否	String	主机quuid
Status	是	否	Uint64	事件状态:0: 待处理 1:忽略 3:已修复 5:检测中， 控制台仅处理0,1,3,5四种状态
Uuid	是	否	String	Uuid
VulId	是	否	Uint64	漏洞id

WebHookRuleDetail

企微机器人规则详情

被如下接口引用：DescribeWebHookRule、ModifyWebHookRule

名称	必选	允许NULL	类型	描述
HookAddr	是	否	String	机器人地址
HostIds	否	否	Array of String	主机Id列表
HostLabels	否	否	Array of WebHookHostLabel	主机范围
IsDisabled	否	否	Int64	是否启用[1:禁用|0:启用]
RuleId	否	否	Int64	规则Id
RuleItems	是	否	Array of WebHookEventKv	事件类型
RuleName	是	否	String	规则名称
RuleRemark	否	否	String	备注信息

AccountStatistics

帐号统计数据。

被如下接口引用：DescribeAccountStatistics

名称	必选	允许NULL	类型	描述
MachineNum	是	否	Uint64	主机数量。
Username	是	否	String	用户名。

AssetDatabaseBaseInfo

资源管理数据库列表信息

被如下接口引用：DescribeAssetDatabaseList

名称	必选	允许NULL	类型	描述
BinPath	否	否	String	二进制路径
ConfigPath	否	否	String	配置文件路径
DataPath	否	否	String	数据路径
ErrorLogPath	否	否	String	错误日志路径
FirstTime	否	否	String	首次采集时间
Id	否	否	String	数据库ID
Ip	否	否	String	绑定IP
IsNew	否	否	Int64	是否新增[0:否|1:是]
LogPath	否	否	String	日志文件路径
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	主机内网IP
MachineName	否	否	String	主机名称
MachineWanIp	否	否	String	主机外网IP
Name	否	否	String	数据库名
OsInfo	否	否	String	操作系统信息
Param	否	否	String	启动参数
Permission	否	否	String	运行权限
PlugInPath	否	否	String	插件路径
Port	否	否	String	监听端口
ProjectId	否	否	Uint64	主机业务组ID
Proto	否	否	String	协议
Quuid	否	否	String	主机Quuid
Tag	否	是	Array of MachineTag	主机标签
UpdateTime	否	是	String	数据更新时间
User	否	否	String	运行用户
Uuid	否	否	String	主机Uuid

名称	必选	允许NULL	类型	描述
Version	否	否	String	版本

BashPolicy

高位命令策略

被如下接口引用：DescribeBashPolicies、ModifyBashPolicy

名称	必选	允许NULL	类型	描述
BashAction	是	否	Int64	0:告警 1:白名单 2:拦截
Category	否	否	Int64	策略类型，0:系统 1:用户
CreateTime	否	否	String	创建时间
DealOldEvents	否	是	Int64	是否处理旧事件为白名单 0=不处理 1=处理
Descript	否	是	String	策略描述
Enable	是	否	Int64	1:有效 0:无效
EventId	否	是	Int64	事件列表点击"加入白名单"时,需要传EventId 事件的id
Id	否	否	Int64	策略ID
Level	是	否	Int64	危险等级(0:无，1: 高危 2:中危 3: 低危)
ModifyTime	否	否	String	修改时间
Name	是	否	String	策略名称
Quuids	否	是	Array of String	生效主机的QUUID集合
Rule	是	否	String	正则表达式
Scope	是	否	Int64	生效范围（0:一组quuid 1:所有专业版(包含旗舰版) 2:所有旗舰版 3:所有主机）
Uuids	否	否	Array of String	老版本兼容可能会用到
White	是	否	Int64	0:黑名单 1:白名单

WebHookRuleSummary

企微机器人规则概要

被如下接口引用：DescribeWebHookRules

名称	必选	允许NULL	类型	描述
CreateTime	否	否	String	创建时间
HookAddr	否	否	String	机器人地址
HostCount	否	否	Int64	主机数目
HostLabels	否	否	Array of WebHookHostLabel	主机范围
IsDisabled	否	否	Int64	是否启用[1:禁用|0:启用]
RuleId	否	否	Int64	规则Id
RuleItems	否	否	Array of WebHookEventKv	事件类型
RuleName	否	否	String	规则名称
RuleRemark	否	否	String	备注信息

名称	必选	允许NULL	类型	描述
UpdateTime	否	否	String	更新时间

BruteAttackList

暴力破解列表

被如下接口引用：

名称	必选	允许NULL	类型	描述
AgentId	是	否	String	AgentId
City	是	否	String	城市
Count	是	否	Uint64	数量
Country	是	否	String	国家
CreateTime	是	否	Datetime_iso	创建时间
EventType	是	否	String	事件类型
HostName	是	否	String	HostName
Id	是	否	String	事件Id
MachineIp	是	否	String	主机IP
MachineName	是	否	String	主机名
Mid	是	否	String	Mid
Province	是	否	String	省份
SrcIp	是	否	String	来源IP
Status	是	否	String	状态
Username	是	否	String	用户名称

IgnoreBaselineRule

忽略的基线检测项信息

被如下接口引用：DescribeIgnoreBaselineRule

名称	必选	允许NULL	类型	描述
EffectHostCount	是	是	Uint64	影响主机数
Fix	是	是	String	修复建议
ModifyTime	是	是	String	更新时间
RuleId	是	是	Uint64	基线检测项id
RuleName	是	是	String	基线检测项名称

BashEventsInfoNew

高危命令数据详情(新)

被如下接口引用：DescribeBashEventsInfoNew

名称	必选	允许NULL	类型	描述
BashCmd	是	否	String	执行命令
CreateTime	是	否	String	发生时间
DetectBy	是	是	Int64	检测来源 0:bash日志 1:实时监控
Exe	是	是	String	进程名称
HarmDescribe	是	是	String	描述
HostIp	是	否	String	主机内网IP
Id	是	否	Uint64	数据ID
MachineName	是	否	String	主机名
MachineStatus	是	是	String	主机在线状态 OFFLINE ONLINE
MachineType	是	是	Int64	0:普通 1:专业版 2:旗舰版
MachineWanIp	是	是	String	主机外网ip
ModifyTime	是	是	String	处理时间
Pid	是	是	String	进程号
Platform	是	否	Uint64	平台类型
PsTree	是	是	String	进程树 json pid:进程id，exe:文件路径 ，account:进程所属用组和用户 ,cmdline:执行命令，ssh_service:SSH服务ip, ssh_soure:登录源
Quuid	是	否	String	主机ID
References	是	是	Array of String	参考链接
RegexBashCmd	是	是	String	自动生成的正则表达式
RuleCategory	是	是	Uint64	规则类别 0=系统规则，1=用户规则
RuleId	是	否	Uint64	规则ID,等于0表示已规则已被删除或生效范围已修改
RuleLevel	是	否	Uint64	规则等级：1-高 2-中 3-低
RuleName	是	否	String	规则名称
Status	是	否	Uint64	处理状态： 0 = 待处理 1= 已处理, 2 = 已加白， 3= 已忽略
SuggestScheme	是	是	String	建议方案
Tags	是	是	Array of String	标签
User	是	是	String	登录用户
Uuid	是	否	String	云镜ID

ImageVirus

容器安全镜像病毒信息

被如下接口引用：

名称	必选	允许NULL	类型	描述
Category	是	否	String	分类
Desc	是	否	String	描述

名称	必选	允许NULL	类型	描述
Path	是	否	String	路径
RiskLevel	是	否	Uint64	风险等级
Tags	是	否	String	标签
VirusName	是	否	String	病毒名称

RiskDnsPolicy

恶意请求策略

被如下接口引用：DescribeRiskDnsPolicyList、ModifyRiskDnsPolicy

名称	必选	允许NULL	类型	描述
Domains	是	否	Array of String	域名,作为入参时需要进行base64 encode
EventId	否	否	Int64	事件ID
HostIds	是	否	Array of String	主机ID
HostScope	是	否	Int64	主机范围[1: 所有专业版+旗舰版|2:所有旗舰版|0: 部分主机]
IsDealOldEvent	否	否	Int64	是否处理之前的事件[0:不处理|1:处理]
IsEnabled	是	否	Int64	是否生效[0:生效,1:不生效]
PolicyAction	是	否	Int64	策略动作[0:告警,1:放行,2:拦截+告警]
PolicyDesc	否	否	String	策略描述
PolicyId	否	否	Int64	策略ID
PolicyName	是	否	String	策略名称
PolicyType	是	否	Int64	策略类型[0:系统,1:用户]
UpdateTime	否	否	String	更新时间

NetAttackTrend

被如下接口引用：DescribeAttackTrends

名称	必选	允许NULL	类型	描述
AttackCount	否	是	Uint64	攻击次数
DateTime	否	是	String	时间点，如 2023-05-06
SuccAttackCount	否	是	Uint64	攻击成功次数
TryAttackCount	否	是	Uint64	尝试攻击次数

MachineClearHistory

机器清理记录对象

被如下接口引用：DescribeMachineClearHistory

名称	必选	允许NULL	类型	描述
AgentLastOfflineTime	是	否	String	客户端最后离线时间

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建时间
Id	是	否	Uint64	ID值
InstanceId	是	否	String	实例ID
InstanceName	是	否	String	实例名称
PrivateIp	是	否	String	内网IP
PublicIp	是	否	String	公网IP

ProtectMachine

机器授权到期信息

被如下接口引用：DescribeWebPageServiceInfo

名称	必选	允许NULL	类型	描述
HostIp	是	否	String	机器IP
HostName	是	否	String	机器名称
SafeguardDirNum	是	否	Uint64	防护目录数

WarningObject

告警更新或插入的参数

被如下接口引用：DescribeSaveOrUpdateWarnings、ModifyWarningSetting

名称	必选	允许NULL	类型	描述
BeginTime	否	否	String	开始时间，格式: HH:mm
ControlBits	否	否	String	漏洞等级控制位二进制，每一位对应页面漏洞等级的开启关闭：低中高（0:关闭；1：开启），例如：101 → 同时勾选低+高；01→(登录审计)疑似不告警，高危告警
DisablePhoneWarning	否	否	Uint64	1: 关闭告警 0: 开启告警
EndTime	否	否	String	结束时间，格式: HH:mm
HostRange	否	是	Int64	告警主机范围类型，0:全部主机，1:按所属项目选，2:按腾讯云标签选，3:按主机安全标签选，4:自选主机
Type	否	否	Uint64	事件告警类型；1：离线，2：木马，3：异常登录，4：爆破，5：漏洞（已拆分为9-12四种类型）6：高位命令，7：反弹sell，8：本地提权，9：系统组件漏洞，10：web应用漏洞，11：应急漏洞，12：安全基线，14：恶意请求，15: 网络攻击，16：Windows系统漏洞，17：Linux软件漏洞

Broadcasts

安全播报列表

被如下接口引用：DescribeSecurityBroadcasts

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	发布时间
Id	是	否	Uint64	文章唯一id
Level	是	否	Uint64	危险程度 0：无， 1：严重， 2: 高危， 3:中危， 4: 低危
Subtitle	是	否	String	副标题

名称	必选	允许NULL	类型	描述
Title	是	是	String	文章名字
Type	是	是	Uint64	类型：0=紧急通知，1=功能更新，2=行业荣誉，3=版本发布

WeeklyReportVul

专业版周报漏洞数据。

被如下接口引用：DescribeWeeklyReportVuls

名称	必选	允许NULL	类型	描述
Description	是	否	String	漏洞描述。
LastScanTime	是	否	Datetime	最后扫描时间。
MachineIp	是	否	String	主机内网IP。
VulName	是	否	String	漏洞名称。
VulStatus	是	否	String	漏洞状态。 - UN_OPERATED : 待处理 - SCANING : 扫描中 - FIXED : 已修复
VulType	是	否	String	漏洞类型。 - WEB : Web漏洞 - SYSTEM :系统组件漏洞 - BASELINE : 安全基线

BaselineItem

基线项

被如下接口引用：DescribeBaselineItemList

名称	必选	允许NULL	类型	描述
CanBeFixed	否	是	Int64	是否可以修复
CategoryId	否	否	Int64	检测项分类
DetectResultDesc	否	是	String	检测结果描述
DetectStatus	否	是	Int64	检测状态：0 未通过，1：忽略，3：通过，5：检测中
FirstTime	否	是	String	第一次出现时间
FixMethod	否	否	String	修复方法
HostId	否	是	String	主机ID
HostIp	否	是	String	主机IP
HostName	否	是	String	主机名
ItemDesc	否	否	String	项描述
ItemId	否	否	Int64	项Id
ItemName	否	否	String	项名称
LastTime	否	是	String	最近出现时间
Level	否	是	Int64	危险等级
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
RuleName	否	否	String	所属规则
Uuid	否	是	String	主机安全uuid
WanIp	否	是	String	外网IP

CKafkaTopicInfo

Ckafka主题名称

被如下接口引用：DescribeLogDeliveryKafkaOptions

名称	必选	允许NULL	类型	描述
TopicID	是	否	String	主题ID
TopicName	是	否	String	主题名称

ProtectPathInfo

主机安全-防护目录信息

被如下接口引用：

名称	必选	允许NULL	类型	描述
Alias	是	否	String	主机名称
AppId	是	是	Uint64	用户Appid
AutoRecover	是	否	Uint64	文件自动恢复开关：0-未开启；1-已启动
Exception	是	否	Uint64	异常，0-无异常，1-超出限制；2-agent离线；3-超时；4-磁盘不足；5-机器已销毁；99-其他
FileTypesWhite	是	否	String	防护文件类型列表，以;分隔
HostIp	是	否	String	主机IP
HostOS	是	否	String	主机操作系统
Id	是	否	Uint64	防护目录ID
Progress	是	否	Uint64	启动进度，百分数不含%
ProtectFileCount	是	否	Uint64	防护文件个数
ProtectPath	是	否	String	防护目录
Quuid	是	否	String	腾迅云CVM uuid
Status	是	否	Uint64	防护状态：0-未开启；1-启动中；2-已启动；3-关闭中；4-已关闭；5-授权到期；6-已删除

VulDefencePluginDetail

单个进程漏洞防御插件状态

被如下接口引用：DescribeVulDefencePluginDetail

名称	必选	允许NULL	类型	描述
ErrorLog	是	否	String	错误日志
InjectLog	是	否	String	注入日志
MainClass	是	否	String	注入进程主类名
Pid	是	否	Int64	注入进程Pid
Status	是	否	Int64	插件状态：0: 注入中, 1: 注入成功, 2: 插件超时, 3: 插件退出, 4: 注入失败 5: 软删除

CKafkaInstanceInfo

CKafka实例信息

被如下接口引用：DescribeLogDeliveryKafkaOptions

名称	必选	允许NULL	类型	描述
Az	是	否	String	地域
Bandwidth	是	否	Int64	实例带宽，单位Mbps
DiskSize	是	否	Int64	磁盘容量，单位GB
Healthy	是	否	Int64	状态，1表示健康，2表示告警，3 表示实例状态异常
InstanceID	是	否	String	实例ID
InstanceName	是	否	String	实例名称
KafkaVersion	是	否	String	版本号
RouteList	是	否	Array of CKafkaRouteInfo	路由列表
SubnetId	是	否	String	子网id
TopicList	是	是	Array of CKafkaTopicInfo	主题列表
VpcId	是	否	String	vpcId，如果为空，说明是基础网络
Zone	是	否	String	可用区

VulFixStatusHostInfo

查看漏洞修复详情 每台主机每个漏洞修复状态

被如下接口引用：DescribeVulFixStatus

名称	必选	允许NULL	类型	描述
FailReason	是	是	String	修复失败原因
HostIp	是	否	String	主机ip
HostName	是	否	String	主机名称
ModifyTime	是	否	String	修复时间
Quuid	是	否	String	主机的quuid
Status	是	否	Uint64	状态：0-初始状态；1-已下发任务（修复中）2-完成（成功）；3-修复失败（失败）4-快照创建失败 导致修复失败（未修复）；

BaselineDetail

基线详情

被如下接口引用：DescribeBaselineDetail

名称	必选	允许NULL	类型	描述
Description	是	是	String	基线描述
Level	是	是	Uint64	危害等级
Name	是	是	String	基线名
PackageName	是	是	String	package名
ParentId	是	是	Uint64	父级id

ScreenBaselineInfo

大屏基线信息

被如下接口引用：DescribeScreenHostInvasion

名称	必选	允许NULL	类型	描述
BaselineFailCount	是	是	Uint64	基线风险项
CategoryId	是	是	Uint64	基线id
LastScanTime	是	是	String	最后检测时间
Level	是	是	Uint64	危害等级：1-低危；2-中危；3-高危；4-严重
Name	是	是	String	基线名
Uuid	是	是	String	主机uuid

VulLevelInfo

漏洞数量按等级分布统计结果实体

被如下接口引用：DescribeVulLevelCount

名称	必选	允许NULL	类型	描述
Count	是	否	Uint64	数量
VulLevel	是	否	Uint64	// 危害等级：1-低危；2-中危；3-高危；4-严重

LicenseBindTaskDetail

授权绑定任务详情

被如下接口引用：DescribeLicenseBindSchedule

名称	必选	允许NULL	类型	描述
ErrMsg	是	否	String	错误信息
Quuid	是	否	String	云服务器UUID
Status	是	否	Uint64	0 执行中, 1 成功,2失败

FileTamperRule

核心文件监控规则

被如下接口引用：DescribeFileTamperEventRuleInfo、DescribeFileTamperRuleInfo、DescribeMachineFileTamperRules、ModifyFileTamperRule

名称	必选	允许NULL	类型	描述
Action	是	否	String	执行动作 跳过：skip，告警：alert
FileAction	是	否	String	文件监控内容 write read read-write
ProcessPath	是	否	String	进程路径
Target	是	否	String	被访问文件路径

BaselineDetectParam

基线扫描参数

被如下接口引用：StartBaselineDetect

名称	必选	允许NULL	类型	描述
HostIds	否	否	Array of String	检测的主机ID集合
ItemIds	否	否	Array of Int64	检测项集合
PolicyIds	否	否	Array of Int64	检测的策略集合
RuleIds	否	否	Array of Int64	检测的规则集合

PrivilegeEscalationProcess

本地提权数据

被如下接口引用：DescribePrivilegeEvents

名称	必选	允许NULL	类型	描述
CmdLine	否	否	String	执行命令
CreateTime	否	否	String	发生时间
FullPath	否	否	String	进程路径
Hostip	否	否	String	主机内网IP
Id	否	否	Uint64	数据ID
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineName	否	否	String	机器名
ParentProcGroup	否	否	String	父进程用户组
ParentProcName	否	否	String	父进程名
ParentProcPath	否	否	String	父进程路径
ParentProcUser	否	否	String	父进程用户名
ProcFilePrivilege	否	否	String	进程文件权限
ProcTree	否	否	String	进程树
ProcessName	否	否	String	进程名
Quuid	否	否	String	主机ID
Status	否	否	Uint64	处理状态：0-待处理 2-白名单 3-已处理 4-已忽略
UserGroup	否	否	String	用户组
UserName	否	否	String	用户名
Uuid	否	否	String	云镜ID

RansomDefenseStrategy

主机列表查询接口相应数据HostList的TagList节点

被如下接口引用：DescribeRansomDefenseStrategyList

名称	必选	允许NULL	类型	描述
BackupType	是	是	Uint64	备份模式： 0按周，1按天

名称	必选	允许NULL	类型	描述
CreateTime	是	是	String	创建时间
Description	是	是	String	策略备注
ExcludeDir	是	是	String	包含目录，用;分隔
Hour	是	否	String	备份执行时间点(0-23): 11:00;12:00
Id	是	否	Int64	策略id
IncludeDir	是	是	String	包含目录，用;分隔
IsAll	是	否	Uint64	是否对所有主机生效
MachineCount	是	是	Uint64	绑定机器数
ModifyTime	是	是	String	最近修改时间
Name	是	否	String	策略名称
SaveDay	是	否	Uint64	保存天数，0永久保存
Status	是	否	Uint64	开启状态：0关闭，1开启
Uin	是	是	String	操作uin
Weekday	是	是	String	备份星期天数（1-7）：1;2;3;4

Malware

木马相关信息

被如下接口引用：DescribeMalwares

名称	必选	允许NULL	类型	描述
Description	是	否	String	木马描述。
FileCreateTime	是	否	Datetime	木马文件创建时间。
FilePath	是	否	String	木马所在的路径。
Id	是	否	Uint64	事件ID。
MachineIp	是	否	String	主机IP。
MachineName	是	否	String	主机名称。
ModifyTime	是	否	Datetime_iso	木马文件修改时间。
Status	是	否	String	当前木马状态。 - UN_OPERATED：未处理 - SEGREGATED：已隔离 - TRUSTED：已信任 - SEPARATING：隔离中 - RECOVERING：恢复中
Uuid	是	否	String	云镜客户端唯一标识UUID。

AssetSystemPackageInfo

资源管理系统安装包列表信息

被如下接口引用：DescribeAssetSystemPackageList

名称	必选	允许NULL	类型	描述
Desc	是	否	String	描述
FirstTime	是	否	String	首次采集时间

名称	必选	允许NULL	类型	描述
InstallTime	是	否	String	安装时间
IsNew	是	否	Int64	是否新增[0:否|1:是]
MachineIp	是	否	String	主机IP
MachineName	是	否	String	主机名称
Name	是	否	String	数据库名
OsInfo	是	否	String	操作系统
Type	是	否	String	类型
UpdateTime	是	是	String	数据更新时间
Version	是	否	String	版本

BaselineRuleType

基线规则类型

被如下接口引用：

名称	必选	允许NULL	类型	描述
TypeId	是	否	Int64	类型Id
TypeName	是	否	String	类型名称

Item

项

被如下接口引用：DescribeBaselineRuleIgnoreList、DescribeBaselineRuleList、ModifyBaselineRule

名称	必选	允许NULL	类型	描述
ItemId	是	否	Int64	Id
ItemName	否	否	String	名称

BanWhiteListDetail

阻断白名单展示列表，包含了机器的信息

被如下接口引用：DescribeBanWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	是	否	Datetime	创建白名单时间
Id	是	否	String	白名单ID
IsGlobal	是	否	Bool	白名单是否全局
MachineIp	是	否	String	机器IP
MachineName	是	否	String	机器名称
ModifyTime	是	否	Datetime	修改白名单时间
Quuid	是	否	String	机器的UUID

名称	必选	允许NULL	类型	描述
Remark	是	否	String	白名单别名
SrcIp	是	否	String	阻断来源IP
Uuid	是	否	String	主机安全程序的UUID

BaselineRuleInfo

基线检测信息

被如下接口引用：DescribeBaselineRule

名称	必选	允许NULL	类型	描述
Description	是	否	String	检测项描述
EventId	是	否	Uint64	唯一事件ID
FixMessage	是	否	String	修复建议
LastScanAt	是	否	String	最后检测时间
Level	是	否	Uint64	危害等级
RuleId	是	否	Uint64	检测项id
RuleName	是	否	String	检测项名称
RuleRemark	是	否	String	具体原因说明
Status	是	否	Uint64	状态
Uuid	是	否	String	唯一Uuid

Account

帐号列表信息数据。

被如下接口引用：DescribeAccounts

名称	必选	允许NULL	类型	描述
AccountCreateTime	是	否	Datetime	帐号创建时间。
Groups	是	否	String	帐号所属组。
Id	是	否	Uint64	唯一ID。
LastLoginTime	是	否	Datetime	帐号最后登录时间。
MachineIp	是	否	String	主机内网IP。
MachineName	是	否	String	主机名称。
Privilege	是	否	String	帐号类型。 - ORDINARY：普通帐号 - SUPPER：超级管理员帐号
Username	是	否	String	帐号名。
Uuid	是	否	String	云镜客户端唯一Uuid

ScreenMachine

大屏主机列表数据

被如下接口引用：DescribeScreenMachines

名称	必选	允许NULL	类型	描述
BaselineNum	否	否	Int64	基线风险数。
CoreVersion	否	否	String	内核版本
CpuLoad	否	否	String	cpu 负载状态
CpuSize	否	否	Float	cpu 核数
CyberAttackNum	否	否	Int64	网络风险数。
DiskLoad	否	否	String	硬盘使用率 %
DiskSize	否	否	Float	硬盘容量GB
InvasionNum	否	否	Int64	入侵事件数
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	主机IP。
MachineName	否	否	String	主机名称。
MachineOs	否	否	String	主机系统。
MachineStatus	否	否	Uint64	大屏主机状态 0：未安装agent，1：离线状态，2:离线-风险，3：离线-严重4：安装设备-正常，5：安装设备-正常 且是专业版或旗舰版，6：安装设备-风险（网络攻击事件>0），7：安装设备-风险（网络攻击事件>0 且是专业版或旗舰版，8：安装设备-严重（入侵检测事件>0），9：安装设备-严重（入侵检测事件>0）且是专业版或旗舰版
MachineType	否	否	String	机器所属专区类型 CVM 云服务器, BM 黑石, ECM 边缘计算, LH 轻量应用服务器 ,Other 混合云专区
MachineWanIp	否	否	String	主机外网IP。
MemLoad	否	否	String	内存负载率%
MemSize	否	否	Float	内存容量 GB
Quuid	否	否	String	CVM或BM机器唯一Uuid。
SecurityStatus	否	否	String	风险状态。 - SAFE：安全 - RISK：风险 - UNKNOWN：未知
Uuid	否	否	String	云镜客户端唯一Uuid，若客户端长时间不在线将返回空字符。
VulNum	否	否	Int64	漏洞数。

AssetAppBaseInfo

资源管理进程基本信息

被如下接口引用：DescribeAssetAppList

名称	必选	允许NULL	类型	描述
BinPath	否	否	String	二进制路径
ConfigPath	否	否	String	配置文件路径
Desc	否	否	String	应用描述
FirstTime	否	否	String	首次采集时间
IsNew	否	是	Int64	是否新增[0:否|1:是]
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	主机内网IP
MachineName	否	否	String	主机名称

名称	必选	允许NULL	类型	描述
MachineWanIp	否	否	String	主机外网IP
Name	否	否	String	应用名称
OsInfo	否	否	String	操作系统信息
ProcessCount	否	否	Uint64	关联进程数
ProjectId	否	否	Uint64	主机业务组ID
Quuid	否	否	String	主机Quuid
Tag	否	是	Array of MachineTag	主机标签
Type	否	否	Uint64	应用类型 1: 运维2 : 数据库3 : 安全4 : 可疑应用5 : 系统架构6 : 系统应用7 : WEB服务99: 其他
UpdateTime	否	是	String	数据更新时间
Uuid	否	否	String	主机Uuid
Version	否	否	String	版本号

BaselineHostTopList

基线影响服务器列表数据

被如下接口引用：DescribeBaselineHostTop

名称	必选	允许NULL	类型	描述
EventLevelList	是	是	Array of BaselineEventLevelInfo	事件等级与次数列表
HostName	是	是	String	主机名称
Quuid	是	是	String	主机Quuid
Score	是	是	Uint64	计算权重的分数

BaselineEventLevelInfo

服务器风险Top的主机信息

被如下接口引用：DescribeBaselineHostTop

名称	必选	允许NULL	类型	描述
EventCount	是	是	Uint64	漏洞数量
EventLevel	是	是	Uint64	危害等级：1-低危；2-中危；3-高危；4-严重

FullTextInfo

全文索引的相关配置

被如下接口引用：DescribeLogIndex

名称	必选	允许NULL	类型	描述
CaseSensitive	是	否	Bool	是否大小写敏感
ContainZH	是	否	Bool	是否包含中文
Tokenizer	是	否	String	分词符

AssetScanTaskHostDetail

描述资产扫描任务中各个主机的任务状态

被如下接口引用：DescribeAssetScanTaskDetail

名称	必选	允许NULL	类型	描述
ErrorMessage	是	否	String	异常信息
MachineIp	是	否	String	主机IP
MachineName	是	否	String	主机名称
Quuid	是	否	String	主机Quuid
Status	是	否	Uint64	任务状态：0进行中，1成功，2失败

BaselineRiskItem

基线检测项top5

被如下接口引用：DescribeBaselineItemRiskTop

名称	必选	允许NULL	类型	描述
HostCount	是	否	Int64	影响服务器数
ItemId	是	是	Int64	检测项Id
ItemName	是	否	String	检测项名字
Level	是	否	Int64	风险等级

BashEventNew

高危命令数据(新)

被如下接口引用：DescribeBashEventsNew

名称	必选	允许NULL	类型	描述
BashCmd	否	否	String	执行命令
CreateTime	否	否	String	发生时间
DetectBy	否	是	Uint64	0: bash日志 1: 实时监控(雷霆版)
Exe	否	是	String	进程名称
HostIp	否	否	String	主机内网IP
Id	否	否	Uint64	数据ID
MachineExtraInfo	否	是	MachineExtraInfo	机器额外信息
MachineName	否	否	String	主机名
MachineType	否	是	Int64	0:普通 1:专业版 2:旗舰版
ModifyTime	否	是	String	处理时间
Pid	否	是	String	进程id
Platform	否	否	Uint64	平台类型
Quuid	否	否	String	主机ID

名称	必选	允许NULL	类型	描述
RegexBashCmd	否	是	String	自动生成的正则表达式
RuleCategory	否	是	Uint64	规则类别 0=系统规则，1=用户规则
RuleId	否	否	Uint64	规则ID
RuleLevel	否	否	Uint64	规则等级：1-高 2-中 3-低
RuleName	否	否	String	规则名称
Status	否	否	Uint64	处理状态： 0 = 待处理 1= 已处理, 2 = 已加白， 3 = 已忽略
User	否	否	String	执行用户名
Uuid	否	否	String	云镜ID

HostLoginWhiteObj

新增登录审计白名单实体

被如下接口引用：AddLoginWhiteLists

名称	必选	允许NULL	类型	描述
EndTime	否	否	String	结束时间
HostInfos	是	否	Array of HostInfo	白名单生效的机器信息列表
IsGlobal	是	否	Uint64	是否对全局生效, 1：全局有效 0: 仅针对单台主机'
Places	是	否	Array of Place	加白地域
Remark	否	否	String	备注
SrcIp	是	否	String	加白源IP，支持网段，多个IP以逗号隔开
StartTime	否	否	String	开始时间
UserName	是	否	String	加白用户名，多个用户名以逗号隔开

ScreenVulInfo

大屏漏洞列表

被如下接口引用：DescribeScreenHostInvasion

名称	必选	允许NULL	类型	描述
Category	是	是	Uint64	漏洞类型 1: web-cms漏洞, 2:应用漏洞, 4: Linux软件漏洞, 5: Windows系统漏洞
Id	是	否	Uint64	漏洞事件id
LastTime	是	否	String	最后检测时间
Level	是	否	Uint64	漏洞等级 1:低 2:中 3:高 4:提示
Name	是	否	String	漏洞名
Uuid	是	是	String	主机UUID
VulId	是	否	Uint64	漏洞id

ProcessStatistics

进程数据统计数据。

被如下接口引用：DescribeProcessStatistics

名称	必选	允许NULL	类型	描述
MachineNum	是	否	Uint64	主机数量。
ProcessName	是	否	String	进程名。

NetAttackTopInfo

被如下接口引用：DescribeAttackTop

名称	必选	允许NULL	类型	描述
Agent	否	是	Array of TopInfo	网络攻击主机维度top统计数据
DstPort	否	是	Array of TopInfo	网络攻击目标端口维度top统计数据
SrcIp	否	是	Array of TopInfo	网络攻击ip来源维度top统计数据
Vul	否	是	Array of TopInfo	网络攻击漏洞维度top统计数据

AssetMachineBaseInfo

资产指纹中服务器列表的基本信息

被如下接口引用：DescribeAssetMachineList

名称	必选	允许NULL	类型	描述
Cpu	否	否	String	CPU信息
CpuLoad	否	否	String	Cpu使用率百分比
CpuSize	否	否	Uint64	Cpu数量
DiskLoad	否	否	String	硬盘使用率百分比
DiskSize	否	否	Uint64	硬盘容量：单位G
FirstTime	否	否	String	首次采集时间
IsNew	否	否	Int64	是否新增[0:否|1:是]
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	服务器内网IP
MachineName	否	否	String	服务器名称
MachineWanIp	否	否	String	主机外网IP
MemLoad	否	否	String	内存使用率百分比
MemSize	否	否	Uint64	内存容量：单位G
OsInfo	否	否	String	操作系统名称
PartitionCount	否	否	Uint64	分区数
ProjectId	否	否	Uint64	业务组ID
Quuid	否	否	String	服务器Quuid
Tag	否	是	Array of MachineTag	标签
UpdateTime	否	是	String	数据更新时间
Uuid	否	否	String	服务器uuid

MalwareListInfo

木马列表集合

被如下接口引用：

名称	必选	允许NULL	类型	描述
Alias	是	否	String	主机别名
CreateTime	是	否	String	创建时间
FileCreateTime	是	否	String	首次运行时间
FileModifierTime	是	否	String	最近运行时间
FilePath	是	否	String	路径
HostIp	是	否	String	服务器ip
Id	是	否	Uint64	唯一ID
LatestScanTime	是	否	String	最近扫描时间
Level	是	否	Uint64	风险等级 0未知、1低、2中、3高、4严重
Status	是	否	Uint64	状态；4-:待处理，5-已信任，6-已隔离，8-文件已删除
Tags	是	否	Array of String	特性标签
Uuid	是	否	String	唯一UUID
VirusName	是	否	String	木马名称

MonthInspectionReport

专家服务-月巡检报告

被如下接口引用：DescribeMonthInspectionReport

名称	必选	允许NULL	类型	描述
ModifyTime	是	否	String	巡检报告更新时间
ReportName	是	否	String	巡检报告名称
ReportPath	是	否	String	巡检报告下载地址

AssetWebLocationInfo

资产管理Web站点列表信息

被如下接口引用：DescribeAssetWebLocationInfo

名称	必选	允许NULL	类型	描述
Command	是	否	String	启动命令
Ip	是	否	String	绑定IP
MainPath	是	否	String	主目录
Name	是	否	String	域名
Port	是	否	String	站点端口
Proto	是	否	String	站点协议

名称	必选	允许NULL	类型	描述
SafeStatus	是	否	Uint64	安全模块状态：0未启用，1启用，999空，仅nginx
ServiceType	是	否	String	服务类型
UpdateTime	是	是	String	数据更新时间
User	是	否	String	运行用户

HostRiskLevelCount

主机风险计数

被如下接口引用：DescribeBaselineHostRiskTop

名称	必选	允许NULL	类型	描述
HighCount	是	否	Int64	高危个数
HostId	是	否	String	主机ID
HostName	是	是	String	主机名
LowCount	是	否	Int64	低危个数
MediumCount	是	否	Int64	中危个数
SeriousCount	是	否	Int64	严重个数

OpenPort

端口列表

被如下接口引用：DescribeOpenPorts

名称	必选	允许NULL	类型	描述
CreateTime	是	否	Datetime	记录创建时间。
Id	是	否	Uint64	唯一ID。
MachineIp	是	否	String	主机IP。
MachineName	是	否	String	主机名。
ModifyTime	是	否	Datetime	记录更新时间。
Pid	是	否	Uint64	端口对应进程Pid。
Port	是	否	Uint64	开放端口号。
ProcessName	是	否	String	端口对应进程名。
Uuid	是	否	String	云镜客户端唯一UUID。

StandardConfig

标准阻断模式的配置

被如下接口引用：

名称	必选	允许NULL	类型	描述
Ttl	是	否	Uint64	阻断时长，单位：秒

OrderResource

订单资源

被如下接口引用：CreateWhiteListOrder

名称	必选	允许NULL	类型	描述
BeginTime	是	否	String	开始时间
EndTime	是	否	String	到期时间
Id	是	否	Uint64	资源主键ID
LicenseType	是	否	Uint64	授权类型
ResourceId	是	否	String	资源ID

SearchTemplate

快速搜索模板

被如下接口引用：CreateSearchTemplate、DescribeSearchTemplates

名称	必选	允许NULL	类型	描述
Condition	是	否	String	检索语句
DisplayData	是	否	String	展示数据
Flag	是	否	String	检索方式。输入框检索：standard,过滤，检索：simple
Id	否	否	Uint64	规则ID
LogType	是	否	String	检索索引类型
Name	是	否	String	检索名称
Query	是	否	String	转换的检索语句内容
TimeRange	是	否	String	时间范围

AssetWebServiceBaseInfo

资源管理Web服务列表信息

被如下接口引用：DescribeAssetWebServiceInfoList

名称	必选	允许NULL	类型	描述
BinPath	否	否	String	二进制路径
ConfigPath	否	否	String	配置路径
Desc	否	否	String	描述
FirstTime	否	否	String	首次采集时间
Id	否	否	String	Web服务ID
InstallPath	否	否	String	安装路径
IsNew	否	否	Int64	是否新增[0:否|1:是]
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	主机内网IP

名称	必选	允许NULL	类型	描述
MachineName	否	否	String	主机名称
MachineWanIp	否	否	String	主机外网IP
Name	否	否	String	数据库名
OsInfo	否	否	String	操作系统信息
ProcessCount	否	否	Uint64	关联进程数
ProjectId	否	否	Uint64	主机业务组ID
Quuid	否	否	String	主机Quuid
Tag	否	是	Array of MachineTag	主机标签
UpdateTime	否	是	String	数据更新时间
User	否	否	String	启动用户
Uuid	否	否	String	主机Uuid
Version	否	否	String	版本

BaselineInfo

基线信息

被如下接口引用：DescribeBaselineList

名称	必选	允许NULL	类型	描述
BaselineFailCount	是	是	Uint64	基线风险项
CategoryId	是	是	Uint64	基线id
HostCount	是	是	Uint64	影响服务器数量
LastScanTime	是	是	String	最后检测时间
Level	是	是	Uint64	危害等级：1-低危；2-中危；3-高危；4-严重
MaxStatus	是	是	Uint64	检测中状态: 5
Name	是	是	String	基线名
RuleCount	是	是	Uint64	检测项数量
Status	是	是	Uint64	通过状态:0:未通过,1:已通过

BaselineWeakPassword

基线弱口令

被如下接口引用：DescribeBaselineWeakPasswordList、ModifyBaselineWeakPassword

名称	必选	允许NULL	类型	描述
CreateTime	否	否	String	创建时间
ModifyTime	否	否	String	修改时间
PasswordId	是	否	Int64	密码Id
WeakPassword	是	否	String	密码

FileTamperRuleCount

主机关联核心文件规则数量信息

被如下接口引用：DescribeFileTamperRuleCount

名称	必选	允许NULL	类型	描述
Count	是	否	Uint64	关联规则的数量
Name	是	是	String	关联规则的名称（仅展示其中一条）
Uuid	是	否	String	主机uuid

ProtectStat

防护信息统计

被如下接口引用：DescribeWebPageProtectStat

名称	必选	允许NULL	类型	描述
Name	是	否	String	名称
Num	是	否	Uint64	数量

VulStoreListInfo

被如下接口引用：DescribeHotVulTop、DescribeVulStoreList

名称	必选	允许NULL	类型	描述
AttackLevel	否	是	Uint64	漏洞攻击热度
CveId	否	是	String	cve编号
FixSwitch	否	是	Uint64	漏洞是否支持自动修复
0-windows/linux均关闭; 1-windows/linux均打开; 2-仅linux; 3-仅windows				
Level	否	是	Uint64	漏洞级别
Method	否	是	Uint64	漏洞检测方法 0 - 版本比对, 1 - POC验证
Name	否	是	String	漏洞名称
PublishDate	否	是	String	发布时间
SupportDefense	否	是	Uint64	漏洞是否支持防御
0:不支持 1:支持				
VulCategory	否	是	Uint64	1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 0= 应急漏洞
VulId	否	是	Uint64	漏洞ID

AssetPortBaseInfo

资源管理账号基本信息

被如下接口引用：DescribeAssetPortInfoList

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
BindIp	否	否	String	绑定IP
FirstTime	否	否	String	首次采集时间
GroupName	否	否	String	所属用户组
IsNew	否	否	Int64	是否新增[0:否|1:是]
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	主机内网IP
MachineName	否	否	String	主机名称
MachineWanIp	否	否	String	主机外网IP
Md5	否	否	String	进程MD5
OsInfo	否	否	String	操作系统信息
Param	否	否	String	启动参数
ParentProcessName	否	否	String	父进程名称
Pid	否	否	String	进程ID
Port	否	否	String	端口
Ppid	否	否	String	父进程ID
ProcessName	否	否	String	进程名称
ProcessPath	否	否	String	进程路径
ProcessVersion	否	否	String	进程版本
ProjectId	否	否	Uint64	主机业务组ID
Proto	否	否	String	端口协议
Quuid	否	否	String	主机Quuid
StartTime	否	否	String	启动时间
Tag	否	是	Array of MachineTag	主机标签
Teletype	否	否	String	进程TTY
UpdateTime	否	是	String	数据更新时间
User	否	否	String	运行用户
Uuid	否	否	String	主机Uuid

PriceDetail

询价参数

被如下接口引用：DescribePrice

名称	必选	允许NULL	类型	描述
GoodsCategoryId	是	否	Uint64	订单分类
GoodsDetail	是	否	String	订单详情参数
GoodsNum	是	否	Uint64	订单数
PayMode	是	否	Uint64	费用模式 0 后付费,1 预付费

名称	必选	允许NULL	类型	描述
RegionId	是	否	Uint64	地域
ZoneId	是	否	Uint64	可用区

WeeklyReport

周报列表。

被如下接口引用：DescribeWeeklyReports

名称	必选	允许NULL	类型	描述
BeginDate	是	否	Date	周报开始时间。
EndDate	是	否	Date	周报结束时间。

MachineTag

服务器标签信息

被如下接口引用：DescribeAssetAppList、DescribeAssetDatabaseList、DescribeAssetMachineList、DescribeAssetPortInfoList、DescribeAssetProcessInfoList、DescribeAssetWebAppList、DescribeAssetWebFrameList、DescribeAssetWebLocationList、DescribeAssetWebServiceInfoList、DescribeImportMachineInfo、DescribeLoginWhiteHostList、DescribeMachineList、DescribeMachines、DescribeMachinesSimple、DescribeRansomDefenseMachineList、DescribeRansomDefenseStrategyMachines

名称	必选	允许NULL	类型	描述
Name	是	否	String	标签名
Rid	是	否	Int64	关联标签ID
TagId	是	否	Uint64	标签ID

BroadcastInfo

安全播报文章详情

被如下接口引用：DescribeSecurityBroadcastInfo

名称	必选	允许NULL	类型	描述
Content	是	否	String	富文本内容信息
CreateTime	是	否	String	发布时间
GotoType	是	是	Uint64	跳转位置：0=不跳转，1=文件查杀，2=漏洞扫描，3=安全基线
Id	是	否	Uint64	文章唯一Id
Subtitle	是	否	String	副标题
Title	是	是	String	文章名字
Type	是	否	Uint64	类型：0=紧急通知，1=功能更新，2=行业荣誉，3=版本发布

JavaMemShellInfo

java内存马事件信息

被如下接口引用：DescribeJavaMemShellList

名称	必选	允许NULL	类型	描述
Alias	否	是	String	服务器名称
CreateTime	否	否	String	首次发现时间
Description	否	否	String	说明
HostIp	否	是	String	服务器IP
Id	否	否	Uint64	事件ID
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
Quuid	否	否	String	服务器quuid
RecentFoundTime	否	否	String	最近检测时间
Status	否	否	Uint64	处理状态 0 -- 待处理 1 -- 已加白 2 -- 已删除 3 - 已忽略 4 - 已手动处理
Type	否	否	Uint64	内存马类型 0:Filter型 1:Listener型 2:Servlet型 3:Interceptors型 4:Agent型 5:其他
Uuid	否	是	String	服务器uuid

UpdateHostLoginWhiteObj

编辑白名单实体

被如下接口引用：ModifyLoginWhiteInfo

名称	必选	允许NULL	类型	描述
EndTime	否	否	String	结束时间
Id	是	否	Uint64	要更新的数据id
Places	是	否	Array of Place	地域信息数组
Remark	是	否	String	备注信息
SrcIp	是	否	String	来源ip
StartTime	否	否	String	开始时间
UserName	是	否	String	用户名

VulInfoList

主机安全-漏洞管理-漏洞列表

被如下接口引用：DescribeVulList

名称	必选	允许NULL	类型	描述
CveId	是	是	String	cve编号
CvssScore	是	是	Float	CVSS评分
DefenseAttackCount	是	是	Uint64	已防御的攻击次数
Descript	是	是	String	描述
DescriptWisteria	是	是	String	废弃字段
FirstAppearTime	是	是	String	首次出现时间
FixSwitch	是	是	Uint64	是否能自动修复且包含能自动修复的主机， 0=否 1=是
From	是	是	Uint64	废弃字段

名称	必选	允许NULL	类型	描述
HostCount	是	否	Uint64	影响主机数
Ids	是	否	String	漏洞包含的事件id串，多个用“,”分割
IsSupportDefense	是	是	Uint64	是否支持防御， 0:不支持 1:支持
Labels	是	是	String	漏洞标签 多个逗号分割
LastTime	是	否	String	最后检测时间
Level	是	否	Uint64	漏洞等级 1:低 2:中 3:高 4:严重
Name	是	否	String	漏洞名
NameWisteria	是	是	String	废弃字段
PublishTime	是	否	String	漏洞披露事件
PublishTimeWisteria	是	是	String	废弃字段
Status	是	否	Uint64	0: 待处理 1:忽略 3:已修复 5:检测中 6:修复中 8:修复失败
StatusStr	是	是	String	聚合后事件状态串
TaskId	是	是	Uint64	最后扫描任务的id
VulCategory	是	是	Uint64	漏洞类别 1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞
VulId	是	否	Uint64	漏洞id

AssetKeyVal

key-val类型的通用数据结构

被如下接口引用：DescribeAssetAppCount、DescribeAssetDatabaseCount、DescribeAssetHostTotalCount、DescribeAssetMachineTagTop、DescribeAssetPortCount、DescribeAssetProcessCount、DescribeAssetRecentMachineInfo、DescribeAssetTotalCount、DescribeAssetTypeTop、DescribeAssetUserCount、DescribeAssetWebAppCount、DescribeAssetWebFrameCount、DescribeAssetWebLocationCount、DescribeAssetWebServiceCount

名称	必选	允许NULL	类型	描述
Desc	是	是	String	描述信息
Key	是	否	String	标签
NewCount	是	是	Int64	今日新增数量
Value	是	否	Int64	数量

ServiceApiInfo

服务及其API列表

被如下接口引用：

名称	必选	允许NULL	类型	描述
ApiList	是	是	Int64	123
ArnDocument	是	是	String	服务介绍文档链接
ConditionKeyList	是	是	Array of String	条件规则列表
Name	是	否	String	服务名称
ServiceType	是	否	String	服务ID

TopInfo

被如下接口引用：DescribeAttackTop

名称	必选	允许NULL	类型	描述
Count	否	是	Uint64	top统计计数
Value	否	是	String	top统计数据，如ip、漏洞名等

JavaMemShellDetail

java内存马事件详细信息

被如下接口引用：DescribeJavaMemShellInfo

名称	必选	允许NULL	类型	描述
Annotations	否	否	String	注释
Args	否	否	String	java进程命令行参数
ClassContent	否	否	String	java内存马二进制代码(base64)
ClassContentPretty	否	否	String	java内存马反编译代码
ClassLoaderName	否	否	String	java加载器类名
ClassName	否	否	String	类名
CreateTime	否	否	String	首次发现时间
Description	否	否	String	说明
EventDescription	否	否	String	事件描述
Exe	否	否	String	java进程路径
InstanceName	否	否	String	容器名
InstanceState	否	否	String	实例状态：RUNNING,STOPPED,SHUTDOWN...
Interfaces	否	否	String	继承的接口
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
MachineState	否	否	String	实例状态：RUNNING,STOPPED,SHUTDOWN...
Md5	否	否	String	类文件MD5
Pid	否	否	Uint64	进程pid
PrivateIp	否	否	String	内网IP
PublicIp	否	否	String	公共ip
RecentFoundTime	否	否	String	最近检测时间
SecurityAdvice	否	否	String	安全建议
Status	否	否	Uint64	处理状态 0 -- 待处理 1 -- 已加白 2 -- 已删除 3 - 已忽略 4 - 已手动处理
SuperClassName	否	否	String	父类名
Type	否	否	Uint64	内存马类型 0:Filter型 1:Listener型 2:Servlet型 3:Interceptors型 4:Agent型 5:其他

Eventlog

安全事件详情

被如下接口引用：DescribeEventlog

名称	必选	允许NULL	类型	描述
Detail	是	否	String	详情原文
EventOperateStatus	是	否	String	事件操作状态
EventStatus	是	否	String	事件状态
EventTime	是	否	String	发生时间
EventType	是	否	String	事件类型
Hostip	是	否	String	主机IP
Id	是	否	String	事件ID
MachineName	是	否	String	主机名
Memo	是	否	String	关键信息
Quuid	是	否	String	主机ID
SeverityClass	是	否	String	威胁等级
Uuid	是	否	String	云镜ID

EventStat

未处理的安全事件统计信息

被如下接口引用：DescribeSecurityEventStat、DescribeStat

名称	必选	允许NULL	类型	描述
EventsNum	是	否	Uint64	事件数
MachineAffectNum	是	否	Uint64	受影响的主机数

RansomDefenseStrategyMachineDetail

防勒索主机列表

被如下接口引用：DescribeRansomDefenseStrategyMachines

名称	必选	允许NULL	类型	描述
CloudTags	是	是	Array of Tag	云标签
DiskInfo	是	是	String	硬盘信息，为空时所有硬盘生效：;分割 diskId1|diskName1;diskId2|diskName2
HostVersion	是	是	Uint64	版本信息：0-基础版 1-专业版 2-旗舰版 3-普惠版
InstanceId	是	否	String	主机实例id
MachineIp	是	否	String	内网ip
MachineName	是	否	String	主机名称
MachineWanIp	是	是	String	外网ip
Quuid	是	否	String	主机Quuid
RegionInfo	是	是	RegionInfo	可用区信息
Status	是	是	Uint64	防护状态：0关闭，1开启
StrategyId	是	是	Uint64	策略id，为0时未绑定策略

名称	必选	允许NULL	类型	描述
StrategyName	是	是	String	策略名称
Tag	是	是	Array of MachineTag	主机安全标签
Uuid	是	否	String	主机Uuid

RiskDnsEvent

恶意请求事件

被如下接口引用：DescribeRiskDnsEventInfo、DescribeRiskDnsEventList

名称	必选	允许NULL	类型	描述
AccessCount	否	否	Int64	访问次数
AgentId	否	否	String	客户端ID
CmdLine	否	否	String	命令行
Domain	否	否	String	访问域名
FirstTime	否	否	String	首次访问时间
HandleStatus	否	否	Int64	处理状态；[0:待处理|2:已加白|3:非信任状态|4:已处理|5:已忽略]
HostId	否	否	String	主机ID
HostIp	否	否	String	主机IP
HostName	否	否	String	主机名称
HostStatus	否	否	String	主机在线状态[OFFLINE:离线|ONLINE:在线|UNKNOWN:未知]
Id	否	否	Int64	事件Id
LastTime	否	否	String	最近访问时间
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
Pid	否	否	Int64	进程ID
PolicyId	否	否	Int64	策略ID
PolicyName	否	否	String	命中策略名称
PolicyType	否	否	Int64	命中策略类型[-1:未知|0系统|1:用户]
ProcessMd5	否	否	String	进程MD5
ProcessName	否	否	String	进程名
ProtectLevel	否	否	Int64	保护级别[0:基础版|1:专业版|2:旗舰版]
ReferenceLink	否	否	String	参考链接
SuggestSolution	否	否	String	修复方案
Tags	否	否	Array of String	标签特性
ThreatDesc	否	否	String	威胁描述
WanIp	否	否	String	外网IP

BaselineCancelParam

基线取消扫描参数

被如下接口引用：

名称	必选	允许NULL	类型	描述
PolicyId	是	否	Int64	取消的策略ID
TaskId	是	否	Int64	取消的任务ID

MachineFileTamperRule

查询主机相关核心文件监控规则详情

被如下接口引用：DescribeMachineFileTamperRules

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	唯一id
Name	是	是	String	规则名称
Rule	是	否	Array of FileTamperRule	规则
RuleCategory	是	否	Uint64	规则类型 0 ：系统规则 1：用户规则

RiskProcessEvent

异常进程事件

被如下接口引用：DescribeRiskProcessEvents

名称	必选	允许NULL	类型	描述
CheckPlatform	否	否	Array of String	木马检测平台 [1:云查杀引擎|2:TAV|3:binaryAi|4:异常行为|5:威胁情报]
CmdLine	否	否	String	执行命令
DetectTime	否	否	String	最近检测时间
EventId	否	否	Int64	事件ID
FilePath	否	否	String	文件路径
HandleStatus	否	否	Int64	处理状态[0待处理;1已处理;2查杀中;3已查杀;4已退出;5忽略]
HostIp	否	否	String	主机IP
HostName	否	否	String	主机名称
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
OnlineStatus	否	否	Int64	主机在线状态
ProcessId	否	否	Int64	进程ID
ReferenceLink	否	否	String	参考链接
StartTime	否	否	String	进程启动时间
SuggestSolution	否	否	String	建议方案
ThreatDesc	否	否	String	威胁描述
Uuid	否	否	String	主机uuid
VirusName	否	否	String	病毒名称
VirusTags	否	否	Array of String	病毒标签
WanIp	否	否	String	外网IP

LoginWhiteListsNew

异地登录白名单

被如下接口引用：DescribeLoginWhiteListNew

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建白名单时间
EndTime	是	是	String	结束时间
HostIp	是	否	String	机器IP
Id	是	否	Uint64	记录ID
IsGlobal	是	否	Uint64	是否为全局规则,1： 全局有效 0: 仅针对单台主机
Locale	是	否	String	地域字符串
MachineName	是	否	String	机器名
ModifyTime	是	否	String	修改白名单时间
Places	是	是	Array of Place	白名单地域
Quuid	是	否	String	主机Quuid
Remark	是	是	String	备注
SrcIp	是	否	String	白名单IP（多个IP逗号隔开）
StartTime	是	是	String	开始时间
UserName	是	否	String	白名单用户（多个用户逗号隔开）
Uuid	是	否	String	云镜客户端ID

AttackSourceEdge

攻击溯源路线描述

被如下接口引用：DescribeAttackSource

名称	必选	允许NULL	类型	描述
From	是	否	String	出发节点
To	是	否	String	目标节点

BruteAttackInfo

密码破解列表实体

被如下接口引用：DescribeBruteAttackList

名称	必选	允许NULL	类型	描述
BanStatus	否	是	Uint64	阻断状态：1-阻断成功；非1-阻断失败
City	否	是	Uint64	城市id
Count	否	是	Uint64	发生次数
Country	否	是	Uint64	国家id
CreateTime	否	是	String	创建时间

名称	必选	允许NULL	类型	描述
DataStatus	否	是	Uint64	0：待处理，1：忽略，5：已处理，6：加入白名单
EventType	否	是	Uint64	事件类型：200-暴力破解事件，300-暴力破解成功事件（页面展示），400-暴力破解不存在的帐号事件
Id	否	否	Uint64	唯一Id
InstanceId	否	是	String	实例ID
IsProVersion	否	是	Bool	是否为专业版（true/false）
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	是	String	主机ip
MachineName	否	是	String	主机名
ModifyTime	否	是	String	最近攻击时间
Port	否	是	Uint64	端口
Protocol	否	是	String	被攻击的服务的用户名
Province	否	是	Uint64	省份id
Quuid	否	是	String	机器UUID
SrcIp	否	是	String	来源ip
Status	否	是	String	SUCCESS：破解成功；FAILED：破解失败
UserName	否	是	String	用户名
Uuid	否	是	String	云镜客户端唯一标识UUID

AssetUserBaseInfo

资源管理账号基本信息

被如下接口引用：DescribeAssetUserList

名称	必选	允许NULL	类型	描述
FirstTime	否	否	String	首次采集时间
Gid	否	否	String	账号GID
HomePath	否	否	String	Home目录
IsDomain	否	否	Uint64	是否域账号：0否， 1是，2否, 999为空 仅windows
IsNew	否	否	Int64	是否新增[0:否|1:是]
IsRoot	否	否	Uint64	是否有root权限：0-否；1是，999为空: 仅linux
IsSshLogin	否	否	Uint64	是否允许ssh登录，1是，0否, 999为空, 仅linux
IsSudo	否	否	Uint64	是否有sudo权限，1是，0否, 999为空, 仅linux
LastLoginTime	否	否	String	上次登录时间
LoginType	否	否	Uint64	登录方式：0-不可登录；1-只允许key登录；2只允许密码登录；3-允许key和密码，999为空，仅linux
MachineExtraInfo	否	是	MachineExtraInfo	
附加信息				
MachineIp	否	否	String	主机内网IP

名称	必选	允许NULL	类型	描述
MachineName	否	否	String	主机名称
MachineWanIp	否	否	String	主机外网IP
Name	否	否	String	账号名称
OsInfo	否	否	String	操作系统信息
PasswordChangeTime	否	否	String	密码修改时间
PasswordDueTime	否	否	String	密码过期时间 仅linux
PasswordLockDays	否	否	Int64	密码锁定时间：单位天, -1为永不锁定 999为空，仅linux
PasswordStatus	否	否	Int64	密码状态：1正常 2即将过期 3已过期 4已锁定 999为空 仅linux
ProjectId	否	否	Uint64	主机业务组ID
Quuid	否	否	String	主机Quuid
Shell	否	否	String	Shell路径 仅linux
ShellLoginStatus	否	否	Uint64	是否shell登录性，0不是；1是 仅linux
Status	否	否	Uint64	账号状态：0-禁用；1-启用
Uid	否	否	String	账号UID
UpdateTime	否	是	String	更新时间
UserType	否	否	Uint64	账号类型：0访客用户，1标准用户，2管理员用户 ,999为空,仅windows
Uuid	否	否	String	主机Uuid

VulFixedInfo

修护的漏洞信息

被如下接口引用：

名称	必选	允许NULL	类型	描述
FixTime	是	否	String	修护时间
FixType	是	否	Uint64	1:快照备份修护，2:直接修护
Level	是	否	Uint64	漏洞等级 1:低 2:中 3:高 4:提示
Name	是	否	String	漏洞名称
VulId	是	否	Uint64	漏洞id

NonLocalLoginPlace

异地登录

被如下接口引用：DescribeNonlocalLoginPlaces

名称	必选	允许NULL	类型	描述
City	是	否	Uint64	城市ID。
Country	是	否	Uint64	国家ID。
Id	是	否	Uint64	事件ID。
LoginTime	是	否	Datetime	登录时间。

名称	必选	允许NULL	类型	描述
MachineIp	是	否	String	主机IP。
MachineName	是	否	String	机器名称。
Province	是	否	Uint64	省份ID。
SrcIp	是	否	String	登录IP。
Status	是	否	String	登录状态 - NON_LOCAL_LOGIN：异地登录 - NORMAL_LOGIN：正常登录
UserName	是	否	String	用户名。
Uuid	是	否	String	云镜客户端唯一标识Uuid。

InsertProtectPathInfo

主机安全-新增文件防护

被如下接口引用：

名称	必选	允许NULL	类型	描述
Fail	是	是	Array of ConfigUUIDInfo	失败的防护目录ID和UUID
Offline	是	是	Array of ConfigUUIDInfo	离线的防护目录ID和UUID
Success	是	是	Array of ConfigUUIDInfo	响应成功的防护目录ID和UUID

BaselineHostDetect

基线主机检测

被如下接口引用：DescribeBaselineHostDetectList

名称	必选	允许NULL	类型	描述
DetectStatus	否	否	Int64	0:未通过 1:忽略 3:通过 5:检测中
FirstTime	否	否	String	首次检测时间
HostId	否	否	String	主机Id
HostIp	否	否	String	内网Ip
HostName	否	否	String	主机名称
ItemCount	否	否	Int64	关联检测项数
LastTime	否	否	String	最后检测时间
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
NotPassedItemCount	否	否	Int64	检测未通过数
PassedItemCount	否	否	Int64	检测通过数
Uuid	否	是	String	主机安全UUID
WanIp	否	否	String	外网Ip

LogHistogram

直方图周期内统计结果详情

被如下接口引用：DescribeLogHistogram

名称	必选	允许NULL	类型	描述
Count	是	否	Int64	统计周期内的日志条数
TimeStamp	是	否	Int64	按 period 取整后的 unix timestamp： 单位毫秒

MachineSnapshotInfo

机器快照信息

被如下接口引用：DescribeMachineSnapshot

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	快照创建时间
DiskId	是	否	String	磁盘id
HostIp	是	否	String	主机ip
HostName	是	否	String	主机名称
InstanceId	是	否	String	实例Id
Quuid	是	否	String	cvm id
RegionId	是	否	Uint64	地区id
SnapshotId	是	否	String	快照id
SnapshotName	是	否	String	快照名称

Tag

标签信息

被如下接口引用：DescribeRansomDefenseMachineList、DescribeRansomDefenseStrategyMachines、DescribeTags

名称	必选	允许NULL	类型	描述
Count	是	否	Uint64	服务器数
Id	是	否	Uint64	标签ID
Name	是	否	String	标签名

ProductStatusInfo

产品试用状态查询接口Data出参

被如下接口引用：DescribeProductStatus

名称	必选	允许NULL	类型	描述
CanApplyTrial	是	否	Bool	是否可以申请试用，true可以申请
CanNotApplyReason	是	否	String	无法试用原因，可试用为空
FWUserStatus	是	否	Uint64	防护状态，1未防护，2防护中，3试用中，4已过期
LastTrialTime	是	否	String	上次试用结束时间（不存在试用记录则为空）

VulFixStatusSnapshotInfo

机器快照信息

被如下接口引用：DescribeVulFixStatus

名称	必选	允许NULL	类型	描述
FailReason	是	是	String	快照创建失败原因
HostIp	是	是	String	主机ip
HostName	是	是	String	主机名称
Id	是	否	Uint64	记录唯一id
ModifyTime	是	是	String	快照创建时间
Quuid	是	否	String	cvm id
SnapshotId	是	是	String	快照id
SnapshotName	是	是	String	快照名称
Status	是	否	Uint64	快照状态 0-初始状态1-快照创建成功；2-快照创建失败；

MalwareRisk

恶意文件风险提示列表信息

被如下接口引用：DescribeMalwareRiskWarning

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	发现时间
Id	是	否	Uint64	唯一ID
MachineIp	是	否	String	机器IP
VirusName	是	否	String	病毒名

ScreenTrendsChart

大屏攻防趋势图

被如下接口引用：DescribeScreenDefenseTrends

名称	必选	允许NULL	类型	描述
Type	是	否	String	统计分类类型 值：防御次数，攻击次数
X	是	否	String	X轴 时间
Y	是	否	Uint64	Y轴 数值

CanFixVulInfo

批量修复漏洞二次弹窗 漏洞主机信息

被如下接口引用：DescribeCanFixVulMachine

名称	必选	允许NULL	类型	描述
FixTag	是	是	Array of String	修复提示tag
HostList	是	是	Array of VulInfoHostInfo	该漏洞可修复的主机信息
VulId	是	是	Uint64	漏洞id

名称	必选	允许NULL	类型	描述
VulName	是	是	String	漏洞名称

AssetJarDetail

资产管理jar包详情

被如下接口引用：DescribeAssetJarInfo

名称	必选	允许NULL	类型	描述
MachineIp	是	否	String	服务器IP
MachineName	是	否	String	服务器名称
Md5	是	是	String	Jar包Md5
Name	是	否	String	名称
OsInfo	是	否	String	操作系统
Path	是	否	String	路径
Process	是	是	Array of AssetAppProcessInfo	引用进程列表
Status	是	否	Uint64	是否可执行：0未知，1是，2否
Type	是	否	Int64	类型：1应用程序，2系统类库，3Web服务自带库，8:其他，
UpdateTime	是	是	String	数据更新时间
Version	是	否	String	版本

VulLevelCountInfo

漏洞等级数量实体

被如下接口引用：DescribeVulHostTop

名称	必选	允许NULL	类型	描述
VulCount	是	否	Uint64	漏洞数量
VulLevel	是	否	Uint64	漏洞等级

VulHostInfo

主机列表响应

被如下接口引用：DescribeHostList

名称	必选	允许NULL	类型	描述
AliasName	是	是	String	主机别名
HostIp	是	是	String	主机IP
IfProfessional	是	是	Bool	是否是专业版主机
Quuid	是	是	String	主机Quuid
TagList	是	是	Array of TagInfo	主机关联的Tag信息
Uuid	是	是	String	主机Uuid

VulEffectModuleInfo

漏洞影响组件详情

被如下接口引用：DescribeVulEffectModules

名称	必选	允许NULL	类型	描述
FixCmd	是	否	String	修复命令
Name	是	否	String	组件名
Path	是	否	String	组件路径
Quuids	是	否	Array of String	影响的主机quuid
Rule	是	否	String	组件影响版本
Uuids	是	否	Array of String	影响的主机uuid
Version	是	否	String	组件版本

ExpertServiceOrderInfo

专家服务订单信息

被如下接口引用：DescribeAvailableExpertServiceDetail、DescribeExpertServiceOrderList

名称	必选	允许NULL	类型	描述
BeginTime	是	否	String	服务开始时间
EndTime	是	否	String	服务结束时间
InquireNum	是	否	Uint64	服务数量
InquireType	是	否	Uint64	订单类型 1应急 2 旗舰重保 3 安全管家
OrderId	是	否	Uint64	订单id
ServiceTime	是	否	Uint64	服务时长几个月
Status	是	否	Uint64	订单状态 0 未启动 1 服务中 2已过期 3完成，4退费销毁

MalwareRiskOverview

文件查杀概览信息

被如下接口引用：DescribeMalwareRiskOverview

名称	必选	允许NULL	类型	描述
FileCount	是	否	Int64	恶意文件数
HostCount	是	否	Int64	影响主机数
IsFirstScan	是	否	Bool	是否首次扫描[false:否|true:是]
ProcessCount	是	否	Int64	异常进程数
ScanTime	是	否	String	最后扫描时间

BaselinePolicyDetect

基线检测策略

被如下接口引用：DescribeBaselineDetectList

名称	必选	允许NULL	类型	描述
FailedCount	是	否	Int64	失败主技数
FinishTime	是	否	String	结束时间
HostCount	是	否	Int64	关联主机数
PolicyDetectStatus	是	是	Int64	1:检测中 2:检测完成
PolicyId	是	否	Int64	策略Id
PolicyName	是	否	String	策略名称
StartTime	是	否	String	开始时间
SuccessCount	是	否	Int64	成功主机数
TaskId	是	否	Int64	检测任务Id
TimeoutCount	是	否	Int64	失败主机数

FileTamperRuleInfo

核心文件监控规则列表

被如下接口引用：DescribeFileTamperRules

名称	必选	允许NULL	类型	描述
AddWhiteType	否	是	String	白名单处理 当前:cur 所有符合历史:all
CreateTime	是	否	String	创建时间
FileAction	是	是	String	FileAction
HostCount	是	是	Uint64	影响主机数
Id	是	否	Uint64	规则id，系统的规则时为0。
IsGlobal	是	否	Uint64	是否是全局的 0：否 ，1：是
Level	是	否	Uint64	风险等级 0：无， 1: 高危， 2:中危， 3: 低危
ModifyTime	是	否	String	更新时间
Name	是	是	String	规则名称
ReadRuleCount	是	否	Uint64	ReadRuleCount
ReadWriteRuleCount	是	否	Uint64	ReadWriteRuleCount
RuleCategory	是	否	Uint64	规则类型 0 ：系统规则 1：用户规则
Status	是	否	Uint64	状态 0: 启用 1: 已关闭
WriteRuleCount	是	否	Uint64	WriteRuleCount

Id

对象id

被如下接口引用：

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	对象id

NetAttackEvent

被如下接口引用：DescribeAttackEvents

名称	必选	允许NULL	类型	描述
Count	否	是	Uint64	攻击次数
DstPort	否	是	Uint64	目标端口
Id	否	是	Uint64	日志ID
Location	否	是	String	来源地
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
MergeTime	否	是	String	攻击时间
New	否	是	Bool	是否今日新增主机
PayVersion	否	是	Uint64	机器付费版本，0 基础版，1专业版，2旗舰版，3普惠版
Quuid	否	是	String	cvm uuid
SrcIP	否	是	String	来源IP
Status	否	是	Uint64	处理状态，0 待处理 1 已处理 2 已加白 3 已忽略 4 已删除 5: 已开启防御
Type	否	是	Uint64	攻击状态，0: 尝试攻击 1: 实锤攻击(攻击成功)
Uuid	否	是	String	客户端ID
VulDefenceStatus	否	是	Uint64	是否开启漏洞防御，0关1开
VulId	否	是	Uint64	漏洞id
VulName	否	是	String	漏洞名称
VulSupportDefense	否	是	Uint64	漏洞是否支持防御，0:不支持 1:支持

JavaMemShellEvent

java内存马事件信息

被如下接口引用：

名称	必选	允许NULL	类型	描述
Alias	是	否	String	服务器名称
Annotations	是	否	String	注释
Args	是	否	String	进程命令行参数
ClassName	是	否	String	类名
CreateTime	是	否	String	首次发现时间
Description	是	否	String	说明
EventDescription	是	否	String	事件描述
Exe	是	否	String	进程路径
HostIp	是	否	String	服务器IP
Interfaces	是	否	String	继承的接口
Md5	是	否	String	类文件MD5
Pid	是	否	Uint64	进程pid

名称	必选	允许NULL	类型	描述
RecentFoundTime	是	否	String	最近检测时间
SecurityAdvice	是	否	String	建议方案
SuperClassName	是	否	String	父类名
Type	是	否	Uint64	内存马类型 0:Filter型 1:Listener型 2:Servlet型 3:Interceptors型 4:Agent型 5:其他

ScreenEventsCnt

统计入侵检测

被如下接口引用：DescribeScreenEventsCnt

名称	必选	允许NULL	类型	描述
Category	是	否	Array of ScreenNameValue	name 具体展示内容类型： 攻击事件, 潜在风险, 失陷资产, 潜在风险资产Value: 事件统计数
Title	是	否	String	展示内容：待处理风险总数，影响资产总数
Total	是	否	Uint64	事件总数

TagMachine

标签相关服务器信息

被如下接口引用：DescribeTagMachines

名称	必选	允许NULL	类型	描述
Id	是	否	String	ID
MachineIp	是	否	String	主机内网IP
MachineName	是	否	String	主机名称
MachineRegion	是	否	String	主机区域
MachineType	是	否	String	主机区域类型
MachineWanIp	是	否	String	主机外网IP
Quuid	是	否	String	主机ID

ReverseShell

反弹Shell数据

被如下接口引用：DescribeReverseShellEvents

名称	必选	允许NULL	类型	描述
CmdLine	否	否	String	命令详情
CreateTime	否	否	String	产生时间
DetectBy	否	否	Uint64	检测方法
DstIp	否	否	String	目标IP
DstPort	否	否	Uint64	目标端口
FullPath	否	否	String	进程路径

名称	必选	允许NULL	类型	描述
Hostip	否	否	String	主机内网IP
Id	否	否	Uint64	ID 主键
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
MachineName	否	否	String	主机名
ParentProcGroup	否	否	String	父进程用户组
ParentProcName	否	否	String	父进程名
ParentProcPath	否	否	String	父进程路径
ParentProcUser	否	否	String	父进程用户
ProcTree	否	否	String	进程树
ProcessName	否	否	String	进程名
Quuid	否	否	String	主机ID
Status	否	否	Uint64	处理状态：0-待处理 2-白名单 3-已处理 4-已忽略
UserGroup	否	否	String	执行用户组
UserName	否	否	String	执行用户
Uuid	否	否	String	云镜UUID

ProtectEventLists

防护事件列表信息

被如下接口引用：DescribeWebPageEventList

名称	必选	允许NULL	类型	描述
CreateTime	否	否	String	发现时间
EventDir	否	否	String	事件地址
EventStatus	否	否	Uint64	事件状态 1 已恢复 0 未恢复
EventType	否	否	Uint64	事件类型 0-内容被修改恢复；1-权限被修改恢复；2-归属被修改恢复；3-被删除恢复；4-新增删除
FileType	否	否	Uint64	文件类型 0-常规文件；1-目录；2-软链
HostIp	否	否	String	服务器ip
HostName	否	否	String	服务器名称
Id	否	否	Uint64	唯一ID
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
RestoreTime	否	否	String	恢复时间

BaselineHost

基线主机信息

被如下接口引用：DescribeBaselineHostIgnoreList、DescribeIgnoreHostAndItemConfig

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
HostId	否	否	String	主机Id
HostIp	否	是	String	内网Ip
HostName	否	是	String	主机名称
HostTag	否	是	String	主机标签
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
WanIp	否	是	String	外网Ip

FieldValueRatioInfo

快速分析统计信息

被如下接口引用：DescribeFastAnalysis

名称	必选	允许NULL	类型	描述
Count	是	否	Int64	个数
Ratio	是	否	Float	比例
Value	是	否	String	值

BaselineEffectHost

基线影响主机信息

被如下接口引用：DescribeBaselineEffectHostList

名称	必选	允许NULL	类型	描述
AliasName	是	是	String	主机别名
FailCount	是	是	Uint64	风险项
FirstScanTime	是	是	String	首次检测事件
HostIp	是	是	String	主机IP
LastScanTime	是	是	String	最后检测时间
MaxStatus	是	是	Uint64	检测中状态
PassCount	是	是	Uint64	通过项
Quuid	是	是	String	主机Quuid
Status	是	是	Uint64	风险项处理状态状态：0-未通过，1-通过
Uuid	是	是	String	主机Uuid

BaselineRuleDetect

基线规则检测

被如下接口引用：DescribeBaselineRuleDetectList

名称	必选	允许NULL	类型	描述
DetectStatus	是	否	Int64	0:未通过 1:忽略 3:通过 5:检测中

名称	必选	允许NULL	类型	描述
FirstTime	是	否	String	首次检测时间
HostCount	是	否	Int64	关联主机数
ItemCount	是	否	Int64	关联项数
ItemIds	是	是	Array of Int64	ItemID集合
LastTime	是	否	String	string
RuleDesc	是	否	String	规则描述
RuleId	是	否	Int64	规则Id
RuleName	是	否	String	规则名称

BaselinePolicy

基线策略信息

被如下接口引用：DescribeBaselinePolicyList、ModifyBaselinePolicy

名称	必选	允许NULL	类型	描述
AssetType	是	否	Int64	资产类型[0:所有专业版旗舰版|1:id|2:ip]
DetectInterval	是	否	Int64	检测间隔[1:1天|3:3天|5:5天|7:7天]
DetectTime	是	否	String	检测时间
HostCount	否	否	Int64	关联基线主机数目
HostIds	否	否	Array of String	主机Id
HostIps	否	否	Array of String	主机Ip
IsDefault	否	否	Int64	是否是系统默认
IsEnabled	是	否	Int64	是否开启[0:未开启|1:开启]
ItemCount	否	否	Int64	关联基线项数目
PolicyId	否	否	Int64	策略Id
PolicyName	是	否	String	策略名称,长度不超过128英文字符
RuleCount	否	否	Int64	关联基线项数目
RuleIds	否	否	Array of Int64	规则Id

VulOverview

漏洞概览

被如下接口引用：DescribeVulOverview

名称	必选	允许NULL	类型	描述
TodayCount	是	否	Int64	今日新增数量
TotalCount	是	否	Uint64	总数

MalwareInfo

恶意文件详情

被如下接口引用：DescribeMalwareInfo

名称	必选	允许NULL	类型	描述
Breadth	否	是	String	影响广度 // 暂时不提供
CheckPlatform	否	是	String	木马检测平台用,分割 1云查杀引擎、2TAV、3binaryAi、4异常行为、5威胁情报
CreateTime	否	否	String	首次发现时间
FileCreateTime	否	否	String	首次运行时间
FileModifierTime	否	否	String	最近一次运行时间
FileName	否	否	String	文件名称
FilePath	否	否	String	文件地址
FileSize	否	否	Int64	文件大小
HarmDescribe	否	否	String	危害描述
Heat	否	是	String	查询热度 // 暂时不提供
HostIp	否	否	String	服务器IP
Id	否	否	Uint64	唯一ID
LatestScanTime	否	否	String	最近扫描时间
Level	否	是	Uint64	风险等级 0提示、1低、2中、3高、4严重
MD5	否	否	String	文件MD5
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineStatus	否	是	String	主机在线状态 OFFLINE ONLINE
MachineWanIp	否	是	String	外网ip
ModifyTime	否	是	String	最近修改时间
ProcessID	否	否	String	进程ID
ProcessName	否	否	String	进程名称
PsTree	否	是	String	进程树 json pid:进程id，exe:文件路径 ，account:进程所属用组和用户 ,cmdline:执行命令，ssh_service: SSH服务ip, ssh_soure:登录源
Reference	否	否	String	参考链接
ServersName	否	否	String	服务器名称
Status	否	是	Uint64	状态；4-:待处理，5-已信任，6-已隔离
StrFileAccessTime	否	是	String	最近访问时间
SuggestScheme	否	否	String	建议方案
Tags	否	否	Array of String	标签特性
Uuid	否	是	String	主机uuid
VirusName	否	否	String	病毒名称

PrivilegeRule

本地提权规则

被如下接口引用：DescribePrivilegeRules

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建时间
Hostip	是	否	String	主机IP
Id	是	否	Uint64	规则ID
IsGlobal	是	否	Uint64	是否全局规则
ModifyTime	是	否	String	修改时间
Operator	是	否	String	操作人
ProcessName	是	否	String	进程名
SMode	是	否	Uint64	是否S权限
Status	是	否	Uint64	状态(0: 有效 1: 无效)
Uuid	是	否	String	客户端ID

RiskDnsList

恶意请求列表

被如下接口引用：DescribeRiskDnsInfo、DescribeRiskDnsList

名称	必选	允许NULL	类型	描述
AccessCount	是	否	Uint64	访问次数
Alias	是	否	String	别名
CmdLine	是	否	String	命令行
CreateTime	是	否	String	首次访问时间
Description	是	否	String	描述
GlobalRuleId	是	否	Uint64	是否为全局规则，0否，1是
HostIp	是	否	String	主机ip
Id	是	否	Uint64	唯一ID
MachineStatus	是	是	String	主机在线状态[OFFLINE:离线|ONLINE:在线|UNKNOWN:未知]
MachineWanIp	是	是	String	外网ip
MergeTime	是	否	String	最近访问时间
Pid	是	否	Uint64	进程号
ProcessMd5	是	否	String	进程MD5
ProcessName	是	否	String	进程名
Quuid	是	否	String	唯一 Quuid
Reference	是	否	String	参考
Status	是	否	Uint64	状态；0-待处理，2-已加白，3-非信任状态，4-已处理，5-已忽略
SuggestScheme	是	否	String	建议方案
Tags	是	否	Array of String	标签特性
Url	是	否	String	对外访问域名
UserRuleId	是	否	Uint64	用户规则id

名称	必选	允许NULL	类型	描述
Uuid	是	否	String	唯一UUID

EffectiveMachineInfo

批量导入机器信息.

被如下接口引用：DescribeImportMachineInfo

名称	必选	允许NULL	类型	描述
CloudTags	否	是	Array of Tags	云标签信息
InstanceID	否	是	String	机器instance ID
KernelVersion	否	是	String	内核版本号
LicenseOrder	否	是	LicenseOrder	授权订单对象
MachineName	否	是	String	机器名称
MachinePrivateIp	否	是	String	机器内网ip
MachinePublicIp	否	是	String	机器公网ip
MachineStatus	否	是	String	在线状态 OFFLINE，ONLINE
MachineTag	否	是	Array of MachineTag	机器标签
Quuid	否	是	String	机器Quuid
Uuid	否	是	String	云镜Uuid
VulNum	否	是	Uint64	漏洞数量

CreateVulFixTaskQuuids

创建修复任务的quuids

被如下接口引用：CreateVulFix

名称	必选	允许NULL	类型	描述
Quuids	是	否	Array of String	需要修复漏洞的主机，所有主机必须有VulId的这个漏洞且是待修复状态。
VulId	是	否	Uint64	漏洞id

ReverseShellRule

反弹Shell规则

被如下接口引用：DescribeReverseShellRules

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建时间
DestIp	是	否	String	目标IP
DestPort	是	否	String	目标端口
Hostip	是	否	String	主机IP
Id	是	否	Uint64	规则ID

名称	必选	允许NULL	类型	描述
IsGlobal	是	否	Uint64	是否全局规则
ModifyTime	是	否	String	修改时间
Operator	是	否	String	操作人
ProcessName	是	否	String	进程名称
Status	是	否	Uint64	状态 (0: 有效 1: 无效)
Uuid	是	否	String	客户端ID

StandardModeConfig

标准模式阻断配置

被如下接口引用：DescribeBanMode

名称	必选	允许NULL	类型	描述
Ttl	是	否	Uint64	阻断时长，单位：秒

AlarmSettingstType

按照类别区分的告警信息

被如下接口引用：

名称	必选	允许NULL	类型	描述
AlarmSettings	是	否	AlarmSettings	告警设置。
Type	是	否	String	告警类型。

AssetPlanTask

资产管理计划任务列表

被如下接口引用：DescribeAssetPlanTaskList

名称	必选	允许NULL	类型	描述
Command	否	否	String	执行命令或脚本
ConfigPath	否	否	String	配置文件路径
Cycle	否	否	String	执行周期
FirstTime	否	否	String	首次采集时间
IsNew	否	否	Int64	是否新增[0:否|1:是]
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	服务器IP
MachineName	否	否	String	服务器名称
MachineWanIp	否	否	String	服务器外网IP
OsInfo	否	否	String	操作系统
Quuid	否	否	String	主机Quuid

名称	必选	允许NULL	类型	描述
Status	否	否	Uint64	默认启用状态：1启用，2未启用
UpdateTime	否	是	String	数据更新时间
User	否	否	String	启动用户
Uuid	否	否	String	主机uuid

ChargePrepaid

预付费模式，即包年包月相关参数设置。通过该参数可以指定包年包月实例的购买时长、是否设置自动续费等属性。

被如下接口引用：InquiryPriceOpenProVersionPrepaid、OpenProVersionPrepaid、RenewProVersion

名称	必选	允许NULL	类型	描述
Period	是	否	Uint64	购买实例的时长，单位：月。取值范围：1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36。
RenewFlag	否	否	String	自动续费标识。取值范围： - NOTIFY_AND_AUTO_RENEW：通知过期且自动续费 - NOTIFY_AND_MANUAL_RENEW：通知过期不自动续费 - DISABLE_NOTIFY_AND_MANUAL_RENEW：不通知过期不自动续费 默认取值：NOTIFY_AND_MANUAL_RENEW。若该参数指定为NOTIFY_AND_AUTO_RENEW，在账户余额充足的情况下，实例到期后将按月自动续费。

BaselineRule

基线规则

被如下接口引用：DescribeBaselineRuleIgnoreList、DescribeBaselineRuleList、ModifyBaselineRule

名称	必选	允许NULL	类型	描述
AssetType	否	是	Int64	[0:所有专业版旗舰版|1:hostID|2:ip]
CategoryId	否	否	Int64	规则分类
HostCount	否	否	Int64	主机数
HostIds	否	是	Array of String	主机Id集合
HostIps	否	是	Array of String	主机IP
Items	否	否	Array of Item	适配项ID列表
RuleDesc	否	否	String	规则描述
RuleId	否	否	Int64	规则Id
RuleName	是	否	String	规则名称,长度不超过128英文字符
RuleType	否	否	Int64	规则类型 [0:系统|1:自定义]

LicenseOrder

授权订单对象内容

被如下接口引用：DescribeImportMachineInfo、DescribeMachinesSimple

名称	必选	允许NULL	类型	描述
LicenseId	是	否	Uint64	授权ID
LicenseType	是	否	Uint64	授权类型

名称	必选	允许NULL	类型	描述
ResourceId	是	否	String	资源ID
SourceType	是	否	Uint64	订单类型
Status	是	否	Uint64	授权订单资源状态

RansomDefenseStrategyMachineBackupInfo

防勒索策略绑定主机备份详情

被如下接口引用：DescribeRansomDefenseMachineList

名称	必选	允许NULL	类型	描述
BackupCount	是	是	Uint64	备份数量
BackupSuccessCount	是	是	Uint64	备份成功次数
CloudTags	是	是	Array of Tag	云标签
DiskInfo	是	是	String	硬盘信息，为空时所有硬盘生效：;分割 diskId1|diskName1;diskId2|diskName2
InstanceId	是	否	String	主机实例id
LastBackupMessage	是	是	String	最近一次备份失败原因
LastBackupStatus	是	是	Uint64	最近一次备份状态：0备份中，1正常，2失败，9暂无备份
LastBackupTime	是	是	String	最近一次备份时间
MachineIp	是	否	String	内网ip
MachineName	是	否	String	主机名称
MachineWanIp	是	是	String	外网ip
Quuid	是	否	String	主机Quuid
RegionInfo	是	是	RegionInfo	可用区信息
RollBackPercent	是	是	Uint64	最近一次回滚进度百分比
RollBackStatus	是	是	Uint64	最近一次回滚状态：0进行中，1成功，2失败
Status	是	是	Uint64	防护状态：0关闭，1开启
StrategyId	是	是	Uint64	策略id，为0时未绑定策略
StrategyName	是	是	String	策略名称
Tag	是	是	Array of MachineTag	主机安全标签
Uuid	是	否	String	主机Uuid

KeyValueInfo

键值索引配置

被如下接口引用：DescribeLogIndex

名称	必选	允许NULL	类型	描述
CaseSensitive	是	否	Bool	是否大小写敏感
KeyValues	是	是	Array of KeyValueArrayInfo	需要建立索引的键值对信息

AssetCoreModuleDetail

资产管理内核模块详情

被如下接口引用：DescribeAssetCoreModuleInfo

名称	必选	允许NULL	类型	描述
Desc	是	否	String	描述
Modules	是	否	String	被依赖模块
Name	是	否	String	名称
Params	是	是	Array of AssetCoreModuleParam	参数信息
Path	是	否	String	路径
Processes	是	否	String	依赖进程
Size	是	否	Uint64	大小
UpdateTime	是	是	String	数据更新时间
Version	是	否	String	版本

OsName

操作系统名称

被如下接口引用：DescribeMachineOsList

名称	必选	允许NULL	类型	描述
MachineOSType	是	否	Uint64	操作系统类型枚举值
Name	是	否	String	系统名称

SecurityEventInfo

安全事件统计列表

被如下接口引用：DescribeSecurityEventsCnt

名称	必选	允许NULL	类型	描述
EventCnt	是	否	Uint64	安全事件数
UuidCnt	是	否	Uint64	受影响机器数

AssetCoreModuleBaseInfo

资产管理内核模块列表

被如下接口引用：DescribeAssetCoreModuleList

名称	必选	允许NULL	类型	描述
Desc	否	否	String	描述
FirstTime	否	否	String	首次采集时间
Id	否	否	String	模块ID
IsNew	否	否	Int64	是否新增[0:否|1:是]

名称	必选	允许NULL	类型	描述
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	服务器IP
MachineName	否	否	String	服务器名称
MachineWanIp	否	否	String	服务器外网IP
ModuleCount	否	否	Uint64	依赖模块数
Name	否	否	String	名称
OsInfo	否	否	String	操作系统
Path	否	否	String	路径
ProcessCount	否	否	Uint64	依赖进程数
Quuid	否	否	String	主机Quuid
Size	否	否	Uint64	模块大小
UpdateTime	否	是	String	数据更新时间
Uuid	否	否	String	主机uuid
Version	否	否	String	版本

BaselineDownload

基线导出结果下载

被如下接口引用：DescribeBaselineDownloadList

名称	必选	允许NULL	类型	描述
DownloadUrl	是	否	String	下载地址
EndTime	是	否	String	完成时间
StartTime	是	否	String	开始时间
Status	是	否	Int64	状态0:未完成 1:完成
TaskId	是	否	Int64	任务Id
TaskName	是	否	String	任务名称

AssetNetworkCardInfo

资产管理网卡信息

被如下接口引用：DescribeAssetMachineDetail、DescribeAssetMachineInfo

名称	必选	允许NULL	类型	描述
DnsServer	是	否	String	DNS服务器
GateWay	是	否	String	网关
Ip	是	否	String	Ipv4对应IP
Ipv6	是	否	String	Ipv6对应IP
Mac	是	否	String	MAC地址
Name	是	否	String	网卡名称

BaselineCategory

基线规则或项的分类

被如下接口引用：DescribeBaselineRuleCategoryList

名称	必选	允许NULL	类型	描述
CategoryId	是	否	Int64	分类Id
CategoryName	是	否	String	分类名称
ParentCategoryId	是	否	Int64	父分类ID,如果为0则没有父分类

LoginWhiteListsRule

白名单规则

被如下接口引用：AddLoginWhiteList、ModifyLoginWhiteList

名称	必选	允许NULL	类型	描述
EndTime	否	否	String	结束时间
HostIp	是	否	String	白名单生效的机器
Id	否	否	Uint64	规则ID，用于更新规则
IsGlobal	是	否	Bool	是否对全局生效
Places	是	否	Array of Place	加白地域
SrcIp	是	否	String	加白源IP，支持网段，多个IP以逗号隔开
StartTime	否	否	String	起始时间
UserName	是	否	String	加白用户名，多个用户名以逗号隔开

ValueInfo

索引的value描述

被如下接口引用：DescribeLogIndex

名称	必选	允许NULL	类型	描述
ContainZH	是	否	Bool	是否包含中文
SqlFlag	是	否	Bool	字段是否开启分析功能
Tokenizer	是	否	String	字段的分词符
Type	是	否	String	字段类型

ProtectNetInfo

专家服务-旗舰护网信息

被如下接口引用：DescribeProtectNetList

名称	必选	允许NULL	类型	描述
EndTime	是	否	String	护网完成时间
ProtectDays	是	否	Uint64	护网天数

名称	必选	允许NULL	类型	描述
ReportPath	是	否	String	报告下载地址
StartTime	是	否	String	护网启动时间
Status	是	否	Uint64	护网状态 0未启动，1护网中，2已完成
TaskId	是	否	String	任务id

FullMachine

主机信息

被如下接口引用：DescribeAllMachines

名称	必选	允许NULL	类型	描述
IsProVersion	是	否	Bool	是否是专业版* true：是* false：否
MachineIp	是	否	String	主机IP。
MachineName	是	否	String	主机名称。
MachineWanIp	是	否	String	主机外网IP。
Quuid	是	否	String	主机唯一标识Uuid。

ImageVul

容器安全镜像漏洞信息

被如下接口引用：

名称	必选	允许NULL	类型	描述
CVEID	是	否	String	漏洞id
CVSSV3Desc	是	否	String	CVSS V3描述
CVSSV3Score	是	否	Float	CVSS V3分数
Category	是	否	String	分类
CategoryType	是	否	String	分类2
Component	是	否	String	组件
DefenseSolution	是	否	String	防御方案
Des	是	否	String	描述
Level	是	否	Uint64	风险等级
Name	是	否	String	漏洞名称
OfficialSolution	是	否	String	解决方案
Reference	是	否	String	引用
SubmitTime	是	否	String	提交时间
Version	是	否	String	版本

BruteAttackRuleList

暴力破解判定规则列表

被如下接口引用：DescribeBruteAttackRules

名称	必选	允许NULL	类型	描述
Enable	是	否	Bool	规则是否为空，为空则填充默认规则
LoginFailTimes	是	否	Uint64	爆破事件失败次数
LoginFailTimesDefault	是	否	Uint64	爆破事件失败次数（默认规则）
TimeRange	是	否	Uint64	爆破事件发生的时间范围，单位：秒
TimeRangeDefault	是	否	Uint64	爆破事件发生的时间范围，单位：秒（默认规则）

Filter

描述键值对过滤器，用于条件过滤查询。例如过滤ID、名称、状态等

若存在多个Filter时，Filter间的关系为逻辑与（AND）关系。 若同一个Filter存在多个Values，同一Filter下Values间的关系为逻辑或（OR）关系。

- 最多只能有5个Filter
- 同一个Filter存在多个Values，Values值数量最多不能超过5个。

被如下接口引用：DescribeAccountStatistics、DescribeAccounts、DescribeAgentVuls、DescribeAssetMachineList、DescribeAssetPortInfoList、DescribeAssetProcessInfoList、DescribeAssetSystemPackageList、DescribeAssetUserList、DescribeAssetWebAppList、DescribeAssetWebFrameList、DescribeAssetWebLocationList、DescribeAttackEvents、DescribeAttackLogs、DescribeAttackTop、DescribeAttackTrends、DescribeBanWhiteList、DescribeBaselineDetectList、DescribeBaselineDownloadList、DescribeBaselineFixList、DescribeBaselineHostDetectList、DescribeBaselineItemDetectList、DescribeBaselineItemIgnoreList、DescribeBaselineItemInfo、DescribeBaselineItemList、DescribeBaselinePolicyList、DescribeBaselineRuleDetectList、DescribeBaselineRuleIgnoreList、DescribeBaselineRuleList、DescribeBaselineWeakPasswordList、DescribeBashEvents、DescribeBashEventsNew、DescribeBashPolicies、DescribeBashRules、DescribeBruteAttackList、DescribeBruteAttacks、DescribeComponentStatistics、DescribeComponents、DescribeEventList、DescribeEventTrend、DescribeEventlog、DescribeExportMachines、DescribeHistoryAccounts、DescribeHostList、DescribeHostLoginList、DescribeIgnoreHostAndItemConfig、DescribeImpactedHosts、DescribeLicenseBindSchedule、DescribeLoginWhiteCombinedList、DescribeLoginWhiteList、DescribeLoginWhiteListNew、DescribeMachineDefenseCnt、DescribeMachineRiskCnt、DescribeMachines、DescribeMachinesSimple、DescribeMalWareList、DescribeMaliciousRequests、DescribeMalwareWhiteList、DescribeMalwareWhiteListAffectList、DescribeMalwares、DescribeNetAttackWhiteList、DescribeNonlocalLoginPlaces、DescribeOpenPortStatistics、DescribeOpenPorts、DescribePrivilegeEvents、DescribePrivilegeRules、DescribeProcessStatistics、DescribeProcesses、DescribeProtectDirRelatedServer、DescribeReverseShellEvents、DescribeReverseShellRules、DescribeRiskDnsEventList、DescribeRiskDnsList、DescribeRiskDnsPolicyList、DescribeRiskProcessEvents、DescribeSecurityEventStat、DescribeVulDefenceEvent、DescribeVulDefenceList、DescribeVulDefencePluginDetail、DescribeVulDefencePluginStatus、DescribeVulEffectHostList、DescribeVulEffectModules、DescribeVulStoreList、DescribeVuls、DescribeWebHookRules、ExportAssetMachineList、ExportAssetPortInfoList、ExportAssetProcessInfoList、ExportAssetSystemPackageList、ExportAssetUserList、ExportAssetWebAppList、ExportAssetWebFrameList、ExportAssetWebLocationList、ExportBaselineFixList、ExportBaselineHostDetectList、ExportBaselineItemDetectList、ExportBaselineItemList、ExportBaselineRuleDetectList、ExportBaselineWeakPasswordList、ExportEventlog、ExportFileTamperRules、ExportJavaMemShellPlugins、ExportJavaMemShells、ExportNonlocalLoginPlaces、ExportRiskDnsEventList、ExportRiskDnsPolicyList、ExportRiskProcessEvents、ExportVulDefenceEvent、ExportVulDefenceList、ExportVulDefencePluginEvent、ExportVulEffectHostList、ExportVulList、ModifyBaselinePolicy、ModifyBaselineRule、ModifyBaselineRuleIgnore

名称	必选	允许NULL	类型	描述
ExactMatch	否	否	Bool	模糊搜索
Name	是	否	String	过滤键的名称。
Values	是	否	Array of String	一个或者多个过滤值。

BaselineRuleTopInfo

基线检测项TOP信息

被如下接口引用：DescribeBaselineTop

名称	必选	允许NULL	类型	描述
EventCount	是	是	Uint64	事件总数

名称	必选	允许NULL	类型	描述
Level	是	是	Uint64	检测项危害等级
RuleId	是	是	Uint64	检测项id
RuleName	是	是	String	基线检测项名

WeeklyReportMalware

专业周报木马数据。

被如下接口引用：DescribeWeeklyReportMalwares

名称	必选	允许NULL	类型	描述
FilePath	是	否	String	木马文件路径。
FindTime	是	否	Datetime	木马发现时间。
MachineIp	是	否	String	主机IP。
Md5	是	否	String	木马文件MD5值。
Status	是	否	String	当前木马状态。 - UN_OPERATED：未处理 - SEGREGATED：已隔离 - TRUSTED：已信任 - SEPARATING：隔离中 - RECOVERING：恢复中

AssetMachineDetail

资产指纹中服务器列表的基本信息

被如下接口引用：DescribeAssetMachineDetail

名称	必选	允许NULL	类型	描述
AgentVersion	否	否	String	agent版本
BootTime	否	否	String	系统启动时间
BuyTime	否	否	String	专业版开通时间
CoreVersion	否	否	String	内核版本
Cpu	否	否	String	CPU信息
CpuLoad	否	否	String	Cpu使用率百分比
CpuLoadVul	否	是	String	CpuLoadVul
CpuSize	否	否	Uint64	Cpu数量
DeviceVersion	否	否	String	设备型号
DiskLoad	否	否	String	硬盘使用率百分比
DiskSize	否	否	Uint64	硬盘容量：单位G
Disks	否	否	Array of AssetDiskPartitionInfo	分区
EndTime	否	否	String	专业版到期时间
FirstTime	否	是	String	FirstTime
InstallTime	否	否	String	安装时间
InstanceId	否	是	String	主机ID
LastLiveTime	否	否	String	最后上线时间

名称	必选	允许NULL	类型	描述
MachineExtraInfo	否	是	MachineExtraInfo	主机二外信息
MachineIp	否	否	String	服务器内网IP
MachineName	否	否	String	服务器名称
MachineWanIp	否	否	String	主机外网IP
MemLoad	否	否	String	内存使用率百分比
MemSize	否	否	Uint64	内存容量：单位G
NetCards	否	否	Array of AssetNetworkCardInfo	网卡
OfflineTime	否	是	String	离线时间
OsInfo	否	否	String	操作系统名称
OsType	否	否	String	linux/windows
PartitionCount	否	否	Uint64	分区数
Producer	否	否	String	生产商
ProjectId	否	否	Uint64	业务组ID
ProtectDays	否	否	Uint64	已防护天数
ProtectLevel	否	否	Uint64	防护级别：0基础版，1专业版，2旗舰版，3普惠版
Quuid	否	否	String	服务器Quuid
RiskStatus	否	否	String	风险状态：UNKNOW-未知，RISK-风险，SAFT-安全
SerialNumber	否	否	String	序列号
Status	否	否	Uint64	0在线，1已离线
UpdateTime	否	是	String	数据更新时间
Uuid	否	否	String	服务器uuid

MachineLicenseDetail

机器绑定授权信息

被如下接口引用：DescribeMachineLicenseDetail

名称	必选	允许NULL	类型	描述
InquireKey	是	否	String	xxx
PayMode	是	否	Uint64	xx
Quuid	是	否	String	主机quuid
ResourceId	是	否	String	xxx
SourceType	是	否	Uint64	xxx

AssetInitServiceBaseInfo

资产管理启动服务列表

被如下接口引用：DescribeAssetInitServiceList

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
FirstTime	否	否	String	首次采集时间
IsNew	否	否	Int64	是否新增[0:否|1:是]
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	服务器IP
MachineName	否	否	String	服务器名称
MachineWanIp	否	否	String	服务器外网IP
Name	否	否	String	名称
OsInfo	否	否	String	操作系统
Path	否	否	String	路径
Quuid	否	否	String	主机Quuid
Status	否	否	Uint64	默认启用状态：0未启用，1启用
Type	否	否	Uint64	类型：1:编码器2:IE插件3:网络提供者4:镜像劫持5:LSA提供者6:KnownDLLs7:启动执行8:WMI9:计划任务10:Winsock提供者11:打印监控器12:资源管理器13:驱动服务14:登录
UpdateTime	否	否	String	数据更新时间
User	否	否	String	启动用户
Uuid	否	否	String	主机uuid

TaskStatus

任务扫描状态列表

被如下接口引用：DescribeScanTaskStatus

名称	必选	允许NULL	类型	描述
Fail	是	否	String	扫描失败
Ok	是	否	String	扫描终止（包含终止中）
Scanning	是	否	String	扫描中（包含初始化）
Stop	是	是	String	扫描失败（提示具体原因：扫描超时、客户端版本低、客户端离线）

NetAttackWhiteRule

被如下接口引用：DescribeNetAttackWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	否	是	String	创建时间
DealOldEvents	否	是	Uint64	是否处理之前的事件 0: 不处理 1:处理
Description	否	是	String	规则描述
Id	否	是	Uint64	规则id
ModifyTime	否	是	String	修改时间
Quuids	否	是	String	主机quuid 多个用;隔开
Scope	否	是	Uint64	0: 一组quuid 1: 所有主机

名称	必选	允许NULL	类型	描述
SrcIP	否	是	String	来源IP 单IP:1.1.1.1 IP范围:1.1.1.1-1.1.2.1 IP范围：1.1.1.0/24 多个用;隔开

ProtectDirInfo

防护目录列表集

被如下接口引用：DescribeProtectDirList

名称	必选	允许NULL	类型	描述
AutoRestoreSwitchStatus	是	否	Uint64	自动恢复开关 (Filters 过滤Quuid 时 返回) 默认0
DirName	是	否	String	网站名称
DirPath	是	否	String	网站防护目录地址
Id	是	否	String	唯一ID
NoProtectServerNum	是	否	Uint64	未防护服务器数
ProtectException	是	否	Uint64	防护异常
ProtectServerNum	是	否	Uint64	防护服务器数
ProtectStatus	是	否	Uint64	防护状态
RelatedServerNum	是	否	Uint64	关联服务器数

HostEvent

主机安全-时间类型列表-测试

被如下接口引用：

名称	必选	允许NULL	类型	描述
Alias	是	否	String	主机名称
AppId	是	否	Uint64	用户ID
ConfigId	是	否	Uint64	防护目录ID
HasRecovered	是	否	Uint64	文件是否已恢复：0-未恢复；1-已恢复
HostIp	是	否	String	主机IP
Id	是	否	Int64	时间主键ID
Path	是	否	String	防护路径
Quuid	是	否	String	CVM uuid
RecoverType	是	否	Uint64	恢复类型
UpdatedAt	是	否	String	恢复时间

ScreenDefendAttackLog

大屏网络攻击日志

被如下接口引用：DescribeScreenHostInvasion

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
CreatedTime	是	否	String	攻击时间
DstIp	是	否	String	目标IP
DstPort	是	否	Uint64	目标端口
HttpMethod	是	否	String	攻击方式
Id	是	否	Uint64	日志ID
Quuid	是	否	String	主机 quuid
SrcIp	是	否	String	来源IP
SrcPort	是	否	Uint64	来源端口
Uuid	是	否	String	客户端ID
VulType	是	否	String	威胁类型

BillingDefineParams

计费下单自定义参数

被如下接口引用：CreateLicenseOrder

名称	必选	允许NULL	类型	描述
AutoBindSwitch	否	否	Bool	自动绑定开关
AutoRepurchaseRenewSwitch	否	否	Bool	自动加购订单是否自动续费
AutoRepurchaseSwitch	否	否	Bool	自动加购开关
ProtectType	否	否	String	防护版本

StrategyDetailInfo

策略详情(包含接口信息)

被如下接口引用：

名称	必选	允许NULL	类型	描述
AddTime	是	否	String	添加时间
Remark	是	是	String	备注
StrategyInfo	是	否	Bool	策略详情
StrategyName	是	否	String	策略名称
StrategyType	是	否	String	策略类型
UpdateTime	是	否	String	更新时间

ReverseShellEventInfo

反弹Shell数据详情

被如下接口引用：DescribeReverseShellEventInfo

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
CmdLine	是	否	String	命令详情
CreateTime	是	否	String	产生时间
DetectBy	是	否	Uint64	检测方法
DstIp	是	否	String	目标IP
DstPort	是	否	Uint64	目标端口
FullPath	是	否	String	进程路径
HarmDescribe	是	否	String	描述
HostIp	是	否	String	主机内网IP
Id	是	否	Uint64	ID 主键
MachineName	是	否	String	主机名
MachineStatus	是	否	String	主机在线状态 OFFLINE ONLINE
MachineWanIp	是	否	String	主机外网ip
ModifyTime	是	否	String	处理时间
ParentProcGroup	是	否	String	父进程用户组
ParentProcName	是	否	String	父进程名
ParentProcPath	是	否	String	父进程路径
ParentProcUser	是	否	String	父进程用户
ProcessName	是	否	String	进程名
PsTree	是	是	String	进程树 json pid:进程id，exe:文件路径 ，account:进程所属用组和用户 ,cmdline:执行命令，ssh_service:SSH服务ip, ssh_soure:登录源
Quuid	是	否	String	主机ID
References	是	否	Array of String	参考链接
Status	是	否	Uint64	处理状态：0-待处理 2-白名单 3-已处理 4-已忽略
SuggestScheme	是	否	String	建议方案
Tags	是	否	Array of String	标签
UserGroup	是	否	String	执行用户组
UserName	是	否	String	执行用户
Uuid	是	否	String	云镜UUID

RuleInfo

索引规则

被如下接口引用：DescribeLogIndex

名称	必选	允许NULL	类型	描述
FullText	是	否	FullTextInfo	全文索引的相关配置
KeyValue	是	否	KeyValueInfo	键值索引的相关配置

名称	必选	允许NULL	类型	描述
Tag	是	否	KeyValueInfo	元字段索引配置

TagInfo

主机列表查询接口相应数据HostList的TagList节点

被如下接口引用：DescribeHostList

名称	必选	允许NULL	类型	描述
TagId	是	是	String	主机TagId
TagName	是	是	String	主机TagName

VulInfoHostInfo

批量修复漏洞二次弹窗

被如下接口引用：DescribeCanFixVulMachine

名称	必选	允许NULL	类型	描述
HostIp	是	是	String	主机ip
HostName	是	是	String	主机名
InstanceId	是	是	String	主机InstanceId
IsSupportAutoFix	是	是	Uint64	0 :漏洞不可自动修复， 1：可自动修复， 2：客户端已离线， 3：主机不是旗舰版只能手动修复， 4：机型不允许 ，5：修复中 ，6：已修复， 7：检测中, 9:修复失败, 10:已忽略 ,11:漏洞只支持linux不支持Windows, 12：漏洞只支持Windows不支持linux
Quuid	是	是	String	主机quuid
Tags	是	是	Array of String	主机标签
Uuid	是	是	String	主机uuid

JavaMemShellPluginSetting

Java内存马插件配置

被如下接口引用：DescribeJavaMemShellPluginList

名称	必选	允许NULL	类型	描述
Alias	是	否	String	服务器名
CreateTime	是	否	String	创建时间
Exception	是	否	Uint64	插件是否存在异常 0: 正常 1: 异常
HostIp	是	否	String	服务器ip
JavaShellStatus	是	否	Uint64	javashell插件开关 0: 关闭 1: 开启
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
ModifyTime	是	否	String	修改时间
Quuid	是	否	String	容器quuid

名称	必选	允许NULL	类型	描述
Uuid	否	是	String	服务器uuid

LogInfo

日志详情

被如下接口引用：SearchLog

名称	必选	允许NULL	类型	描述
Content	是	否	String	日志内容的Json序列化字符串
FileName	是	否	String	日志文件名称
Source	是	否	String	日志来源IP
TimeStamp	是	否	Int64	日志时间，单位ms

AssetUserDetail

资源管理账号基本信息

被如下接口引用：DescribeAssetUserInfo

名称	必选	允许NULL	类型	描述
DisableTime	是	否	String	账号到期时间
Gid	是	否	String	账号GID
GroupName	是	否	String	用户组名
HomePath	是	否	String	Home目录
IsDomain	是	否	Uint64	是否域账号：0否， 1是, 999为空 仅windows
IsRoot	是	否	Uint64	是否有root权限：0-否；1是，999为空: 仅linux
IsSshLogin	是	否	Uint64	是否允许ssh登录，1是，0否, 999为空, 仅linux
Keys	是	是	Array of AssetUserKeyInfo	用户公钥列表
LastLoginIp	是	否	String	最近登录IP
LastLoginLoc	是	否	String	最近登录位置
LastLoginTerminal	是	否	String	最近登录终端
LastLoginTime	是	否	String	上次登录时间
MachineIp	是	否	String	主机内网IP
MachineName	是	否	String	主机名称
Name	是	否	String	账号名称
PasswordChangeTime	是	否	String	密码修改时间
PasswordChangeType	是	否	Uint64	密码修改设置：0-不可修改，1-可修改
PasswordDueTime	是	否	String	密码过期时间 仅linux
PasswordLockDays	是	否	Int64	密码锁定时间：单位天, -1为永不锁定 999为空，仅linux
PasswordWarnDays	是	否	Uint64	密码过期提醒：单位天
Quuid	是	否	String	主机Quuid

名称	必选	允许NULL	类型	描述
Remark	是	否	String	备注
Shell	是	否	String	Shell路径 仅linux
ShellLoginStatus	是	否	Uint64	是否shell登录性，0不是；1是 仅linux
Status	是	否	Uint64	账号状态：0-禁用；1-启用
Uid	是	否	String	账号UID
UpdateTime	是	是	String	数据更新时间
UserType	是	否	Uint64	账号类型：0访客用户，1标准用户，2管理员用户 ,999为空,仅windows
Uuid	是	否	String	主机Uuid

AssetWebFrameBaseInfo

资源管理Web应用列表信息

被如下接口引用：DescribeAssetWebFrameList

名称	必选	允许NULL	类型	描述
FirstTime	否	否	String	首次采集时间
IsNew	否	否	Int64	是否新增[0:否|1:是]
Lang	否	否	String	语言
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	主机内网IP
MachineName	否	否	String	主机名称
MachineWanIp	否	否	String	主机外网IP
Name	否	否	String	数据库名
OsInfo	否	否	String	操作系统信息
ProjectId	否	否	Uint64	主机业务组ID
Quuid	否	否	String	主机Quuid
ServiceType	否	否	String	服务类型
Tag	否	是	Array of MachineTag	主机标签
UpdateTime	否	是	String	数据更新时间
Uuid	否	否	String	主机Uuid
Version	否	否	String	版本

HostTagInfo

主机与主机标签信息

被如下接口引用：DescribeHostInfo

名称	必选	允许NULL	类型	描述
AliasName	否	是	String	主机名
CloudTags	否	是	Array of Tags	云标签信息

名称	必选	允许NULL	类型	描述
HostIp	否	是	String	主机内网Ip
InstanceID	否	是	String	主机instance ID
KernelVersion	否	是	String	内核版本号
MachineStatus	否	是	String	主机在线状态 ONLINE，OFFLINE
MachineWanIp	否	是	String	主机公网ip
ProtectType	否	是	String	防护版本 BASIC_VERSION 基础版, PRO_VERSION 专业版 Flagship 旗舰版
Quuid	否	是	String	主机Quuid
TagList	否	是	Array of String	主机标签名数组
Uuid	否	是	String	主机uuid
VulNum	否	是	Int64	漏洞数

MaliciousRequest

恶意请求数据。

被如下接口引用：DescribeMaliciousRequests

名称	必选	允许NULL	类型	描述
CmdLine	是	否	String	执行命令行。
Count	是	否	Uint64	恶意请求数。
CreateTime	是	否	Datetime	发现时间。
Description	是	否	String	恶意请求域名描述。
Domain	是	否	String	恶意请求域名。
Id	是	否	Uint64	记录ID。
MachineIp	是	否	String	主机内网IP。
MachineName	是	否	String	主机名。
MergeTime	是	否	Datetime	记录合并时间。
Pid	是	否	Uint64	进程PID。
ProcessMd5	是	否	String	进程MD5值。
ProcessName	是	否	String	进程名。
Reference	是	否	String	参考地址。
Status	是	否	String	记录状态。 - UN_OPERATED：待处理 - TRUSTED：已信任 - UN_TRUSTED：已取消信任
Uuid	是	否	String	云镜客户端UUID。

AgentVul

主机漏洞信息

被如下接口引用：DescribeAgentVuls

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
Description	是	否	String	漏洞描述。
Id	是	否	Uint64	漏洞ID。
LastScanTime	是	否	Datetime	最后扫描时间。
MachineIp	是	否	String	主机IP。
VulId	是	否	Uint64	漏洞种类ID。
VulLevel	是	否	String	漏洞危害等级。 - HIGH：高危 - MIDDLE：中危 - LOW：低危 - NOTICE：提示
VulName	是	否	String	漏洞名称。
VulStatus	是	否	String	漏洞状态。 - UN_OPERATED：待处理 - FIXED：已修复

PrivilegeEventInfo

本地提权数据

被如下接口引用：DescribePrivilegeEventInfo

名称	必选	允许NULL	类型	描述
CmdLine	是	否	String	执行命令
CreateTime	是	否	String	发生时间
FullPath	是	否	String	进程路径
HarmDescribe	是	否	String	危害描述信息
HostIp	是	否	String	主机内网IP
Id	是	否	Uint64	数据ID
MachineName	是	否	String	机器名
MachineStatus	是	否	String	主机在线状态 OFFLINE ONLINE
MachineWanIp	是	否	String	主机外网ip
ModifyTime	是	否	String	处理时间
NewCaps	是	否	String	权限列表|隔开
ParentProcGroup	是	否	String	父进程用户组
ParentProcName	是	否	String	父进程名
ParentProcPath	是	否	String	父进程路径
ParentProcUser	是	否	String	父进程用户名
ProcFilePrivilege	是	否	String	进程文件权限
ProcessName	是	否	String	进程名
PsTree	是	否	String	进程树 json pid:进程id，exe:文件路径 ，account:进程所属用组和用户 ,cmdline:执行命令，ssh_service:SSH服务ip, ssh_soure:登录源
Quuid	是	否	String	主机ID
References	是	否	Array of String	参考链接
Status	是	否	Uint64	处理状态：0-待处理 2-白名单 3-已处理 4-已忽略

名称	必选	允许NULL	类型	描述
SuggestScheme	是	否	String	建议方案
Tags	是	否	Array of String	标签
UserGroup	是	否	String	用户组
UserName	是	否	String	用户名
Uuid	是	否	String	云镜ID

MalwareWhiteListInfo

木马白名单信息

被如下接口引用：DescribeMalwareWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	规则创建时间
EventsCount	是	否	Uint64	受影响记录
FileDirectory	是	否	String	文件目录；按,分割
FileExtension	是	否	String	文件后缀；按,分割
FileName	是	否	String	文件名；按,分割
Id	是	否	Uint64	唯一ID。
IsGlobal	是	否	Uint64	是否全部主机； 0否，1是
MatchType	是	否	Uint64	匹配模式；0精确匹配，1模糊匹配
Md5List	是	否	String	md5列表 按,分割
Mode	是	否	Uint64	白名单模式；0 MD5 ，1自定义
QuuidList	是	否	String	cvm quuid 按,分割。

HistoryAccount

账号变更历史数据。

被如下接口引用：DescribeHistoryAccounts

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	唯一ID。
MachineIp	是	否	String	主机内网IP。
MachineName	是	否	String	主机名。
ModifyTime	是	否	Datetime	变更时间。
ModifyType	是	否	String	帐号变更类型。 - CREATE：表示新增帐号 - MODIFY：表示修改帐号 - DELETE：表示删除帐号
Username	是	否	String	帐号名。
Uuid	是	否	String	云镜客户端唯一Uuid。

AssetCoreModuleParam

资产管理内核模块参数

被如下接口引用：DescribeAssetCoreModuleInfo

名称	必选	允许NULL	类型	描述
Data	是	否	String	数据
Name	是	否	String	名称

Filters

描述键值对过滤器，用于条件过滤查询。例如过滤ID、名称、状态等

若存在多个Filter时，Filter间的关系为逻辑与（AND）关系。 若同一个Filter存在多个Values，同一Filter下Values间的关系为逻辑或（OR）关系。

被如下接口引用：DescribeBaselineEffectHostList、DescribeBaselineList、DescribeCanNotSeparateMachine、DescribeEmergencyResponseList、DescribeEmergencyVulList、DescribeExpertServiceList、DescribeExpertServiceOrderList、DescribeFileTamperEvents、DescribeFileTamperRules、DescribeIgnoreRuleEffectHostList、DescribeImportMachineInfo、DescribeJavaMemShellList、DescribeJavaMemShellPluginInfo、DescribeJavaMemShellPluginList、DescribeLicenseBindList、DescribeLicenseList、DescribeMachineClearHistory、DescribeMaliciousRequestWhiteList、DescribeProtectNetList、DescribeRansomDefenseBackupList、DescribeRansomDefenseEventsList、DescribeRansomDefenseMachineList、DescribeRansomDefenseRollBackTaskList、DescribeRansomDefenseStrategyList、DescribeRansomDefenseStrategyMachines、DescribeScanState、DescribeScanTaskDetails、DescribeTags、DescribeVulList、ExportAttackEvents、ExportAttackLogs、ExportBaselineEffectHostList、ExportBaselineList、ExportBashEvents、ExportBashEventsNew、ExportBashPolicies、ExportBruteAttacks、ExportFileTamperEvents、ExportIgnoreRuleEffectHostList、ExportLicenseDetail、ExportMaliciousRequests、ExportMalwares、ExportPrivilegeEvents、ExportRansomDefenseBackupList、ExportRansomDefenseEventsList、ExportRansomDefenseMachineList、ExportRansomDefenseStrategyList、ExportRansomDefenseStrategyMachines、ExportReverseShellEvents、ExportScanTaskDetails、ExportVulDetectionReport、ModifyEventAttackStatus、ModifyRiskEventsStatus、OpenProVersionActivity

名称	必选	允许NULL	类型	描述
ExactMatch	否	否	Bool	是否模糊匹配，前端框架会带上，可以不管
Name	是	否	String	过滤键的名称。
Values	是	否	Array of String	一个或者多个过滤值。

AssetType

资产指纹类型描述

被如下接口引用：DescribeAssetTypes

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	类型ID
Name	是	否	String	类型名称

VulDefenceRangeDetail

漏洞防御范围详情

被如下接口引用：DescribeVulDefenceList

名称	必选	允许NULL	类型	描述
CveId	是	否	String	cve id
CvssScore	是	否	Float	cvss 分数
Label	是	否	String	标签
Level	是	否	Uint64	漏洞级别： 1低危 2中危 3高危 4严重

名称	必选	允许NULL	类型	描述
PublishTime	是	否	String	发布时间
VulId	是	否	Int64	漏洞id
VulName	是	否	String	漏洞名称

JavaMemShellPluginStatus

java内存马插件状态信息

被如下接口引用：

名称	必选	允许NULL	类型	描述
Alias	是	否	String	服务器名
ErrorLog	是	否	String	错误日志
HostIp	是	否	String	服务器ip
MainClass	是	否	String	注入进程主类名
Pid	是	否	Uint64	注入进程pid
Status	是	否	Uint64	插件状态：0: 注入中, 1: 注入成功, 2: 插件超时, 3: 插件退出, 4: 注入失败 5: 软删除

VulTopInfo

漏洞top统计实体

被如下接口引用：DescribeVulTop

名称	必选	允许NULL	类型	描述
VulCount	是	是	Uint64	漏洞数量
VulId	是	是	Uint64	漏洞id
VulLevel	是	是	Uint64	危害等级：1-低危；2-中危；3-高危；4-严重
VulName	是	是	String	漏洞 名

VulDetailInfo

漏洞详细信息

被如下接口引用：DescribeScanTaskDetails

名称	必选	允许NULL	类型	描述
CveId	是	否	String	cve编号
Cvss	是	否	String	CVSS详情
CvssScore	是	否	Float	CVSS评分
Descript	是	否	String	漏洞描述
Fix	是	否	String	修复建议
Level	是	否	Uint64	漏洞级别
Name	是	否	String	漏洞名称

名称	必选	允许NULL	类型	描述
PublishTime	是	否	String	发布时间
Reference	是	否	String	参考链接
VulCategory	是	否	Uint64	1: web-cms漏洞 2:应用漏洞 4: Linux软件漏洞 5: Windows系统漏洞 0= 应急漏洞
VulId	是	否	Uint64	漏洞ID

WarningInfoObj

告警设置列表

被如下接口引用：DescribeWarningList

名称	必选	允许NULL	类型	描述
BeginTime	是	否	String	开始时间，格式: HH:mm
ControlBit	是	否	Uint64	漏洞等级控制位（对应DB的十进制存储）
ControlBits	是	否	String	漏洞等级控制位二进制，每一位对应页面漏洞等级的开启关闭：低中高（0:关闭；1：开启），例如：101 → 同时勾选低+高
Count	是	是	Int64	配置的告警范围主机个数，前端用此判断展示提示信息
DisablePhoneWarning	是	否	Uint64	1: 关闭告警 0: 开启告警
EndTime	是	否	String	结束时间，格式: HH:mm
HostRange	否	是	Int64	告警主机范围类型，0:全部主机，1:按所属项目选，2:按腾讯云标签选，3:按主机安全标签选，4:自选主机
OfflineInterval	是	是	Int64	离线类型判断时间 单位秒
TimeZone	是	否	String	时区信息
Type	是	否	Uint64	事件告警类型；1：离线，2：木马，3：异常登录，4：爆破，5：漏洞（已拆分为9-12四种类型）6：高危命令，7：反弹sell，8：本地提权，9：应用漏洞，10：web-cms漏洞，11：应急漏洞，12：安全基线,13: 防篡改，14：恶意请求，15: 网络攻击，16：Windows系统漏洞，17：Linux软件漏洞，18：核心文件监控告警，19：客户端卸载告警。20：客户端离线告警

KeyValueArrayInfo

索引键值信息

被如下接口引用：DescribeLogIndex

名称	必选	允许NULL	类型	描述
Key	是	否	String	需要配置键值或者元字段索引的字段
Value	是	否	ValueInfo	字段的索引描述信息

AssetWebLocationBaseInfo

资产管理Web站点列表信息

被如下接口引用：DescribeAssetWebLocationList

名称	必选	允许NULL	类型	描述
FirstTime	否	否	String	首次采集时间
Id	否	否	String	Web站点Id

名称	必选	允许NULL	类型	描述
IsNew	否	是	Int64	是否新增[0:否|1:是]
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	内网IP
MachineName	否	否	String	主机名称
MachineWanIp	否	否	String	外网IP
MainPath	否	否	String	主目录
MainPathOwner	否	否	String	主目录所有者
Name	否	否	String	域名
OsInfo	否	否	String	操作系统
PathCount	否	否	Uint64	站点路经数
Permission	否	否	String	拥有者权限
Port	否	否	String	站点端口
ProjectId	否	否	Uint64	主机业务组ID
Proto	否	否	String	站点协议
Quuid	否	否	String	主机Quuid
ServiceType	否	否	String	服务类型
Tag	否	否	Array of MachineTag	主机标签
UpdateTime	否	是	String	数据更新时间
User	否	否	String	运行用户
Uuid	否	否	String	主机Uuid

ScreenRegionMachines

大屏主机3D图 列表

被如下接口引用：DescribeScreenMachines

名称	必选	允许NULL	类型	描述
AttackCnt	是	否	Uint64	潜在风险主机数
IgnoreCnt	是	否	Uint64	省略展示多少主机，等于0时没有省略展示
Machines	是	否	Array of ScreenMachine	主机列表
Region	是	否	String	所有区域
RegionName	是	否	String	区域中文描述
RiskCnt	是	否	Uint64	风险主机数量
SafetyCnt	是	否	Uint64	无风险主机数
TotalCount	是	否	Uint64	此区域的主机总数
UnAgentOfflineCnt	是	否	Uint64	离线/未安装主机数

Vul

漏洞列表数据

被如下接口引用：DescribeVuls

名称	必选	允许NULL	类型	描述
ImpactedHostNum	是	否	Uint64	受影响机器数量
LastScanTime	是	否	Datetime	最后扫描时间
VulId	是	否	Uint64	漏洞种类ID
VulLevel	是	否	String	漏洞危害等级:HIGH：高危MIDDLE：中危LOW：低危NOTICE：提示
VulName	是	否	String	漏洞名称
VulStatus	是	否	String	漏洞状态* UN_OPERATED：待处理* FIXED：已修复

RansomDefenseBackup

主机快照备份列表

被如下接口引用：DescribeRansomDefenseBackupList

名称	必选	允许NULL	类型	描述
BackupStatus	是	否	Uint64	备份状态：0备份中，1正常，2、3失败，4快照已过期，9快照已删除
BackupTime	是	否	String	备份时间
DiskCount	是	否	Uint64	备份磁盘数量
Disks	是	否	String	硬盘信息，；分隔
EventStatus	是	否	Uint64	勒索状态：0无告警, 1有告警
SnapshotIds	是	否	String	快照列表，；分隔
StrategyId	是	否	Uint64	策略id
StrategyName	是	否	String	策略名称
StrategyStatus	是	否	Uint64	策略状态:0关闭，1开启，9已删除

AssetLoadSummary

资源负载概况

被如下接口引用：DescribeAssetLoadInfo

名称	必选	允许NULL	类型	描述
Counts	是	否	Array of Uint64	负载量数组，依次为：[0%或未知数量，0%～20%，20%～50%，50%～80%，80%～100%]
Top5	是	是	Array of AssetLoadDetail	负载Top5

EmergencyVul

应急漏洞信息

被如下接口引用：DescribeEmergencyVulList

名称	必选	允许NULL	类型	描述
Category	是	否	Uint64	漏洞分类
CveId	是	是	String	cve编号

名称	必选	允许NULL	类型	描述
CvssScore	是	是	Float	CVSS评分
DefenseAttackCount	是	是	Uint64	已防御的攻击次数
HostCount	是	是	Uint64	影响机器数
IsSupportDefense	是	是	Uint64	是否支持防御， 0:不支持 1:支持
Labels	是	是	String	漏洞标签 多个逗号分割
LastScanTime	是	否	String	最后扫描时间
Level	是	否	Uint64	漏洞级别
Progress	是	否	Uint64	扫描进度
PublishDate	是	否	String	发布日期
Status	是	否	Uint64	漏洞状态 0未检测 1有风险 ，2无风险 ，3 检查中展示progress
VulId	是	否	Uint64	漏洞id
VulName	是	否	String	漏洞名称

MachineInfo

单个机器的详细信息

被如下接口引用：

名称	必选	允许NULL	类型	描述
MachineIp	是	否	String	机器ip。
ProtectDays	是	否	Uint64	保护天数。
ProtectLevel	是	否	Uint64	防护级别。
Region	是	否	String	地域。
RegionType	是	否	String	类型：bm或者cvm。
VipOpenTime	是	否	Date	专业版开通时间。

LoginWhiteLists

异地登录白名单

被如下接口引用：DescribeLoginWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	是	否	Datetime	创建白名单时间
EndTime	是	否	String	结束时间
HostIp	是	否	String	机器IP
Id	是	否	Uint64	记录ID
IsGlobal	是	否	Bool	是否为全局规则
MachineName	是	否	String	机器名
ModifyTime	是	否	Datetime	修改白名单时间
Places	是	否	Array of Place	白名单地域

名称	必选	允许NULL	类型	描述
SrcIp	是	否	String	白名单IP（多个IP逗号隔开）
StartTime	是	否	String	起始时间
UserName	是	否	String	白名单用户（多个用户逗号隔开）
Uuid	是	否	String	云镜客户端ID

AgentVuls

主机详情漏洞列表

被如下接口引用：

名称	必选	允许NULL	类型	描述
Description	是	否	String	漏洞描述
HostIp	是	否	String	主机IP
Id	是	否	Uint64	漏洞ID
LastScanTime	是	否	Datetime	最后扫描时间
VulId	是	否	Uint64	漏洞种类ID
VulLevel	是	否	String	漏洞危害等级:HIGH：高危MIDDLE：中危LOW：低危NOTICE：提示
VulName	是	否	String	漏洞名称

OrderModifyObject

订单变配参数对象

被如下接口引用：CreateLicenseOrder

名称	必选	允许NULL	类型	描述
InquireNum	否	否	Int64	扩容/缩容数,变配子产品忽略该参数
NewSubProductCode	否	否	String	新产品标识,这里支持PRO_VERSION 专业版,FLAGSHIP 旗舰版
ResourceId	否	否	String	资源ID

AttackSourceNode

攻击溯源节点

被如下接口引用：DescribeAttackSource

名称	必选	允许NULL	类型	描述
EndTime	是	否	String	结束时间
EventId	是	否	Uint64	事件ID，为空的时候表示没有对应事件
EventType	是	否	String	BRUTEFORCE:密码破解、MALWARE:木马、BASH:高危命令、RISK_DNS:恶意请求、LOGIN:异地登录、HOST:主机节点, TIME_ORDER：通用节点
Ip	是	否	String	节点ip 当节点为HOST时
Level	是	否	Uint64	等级 0：提示，1：低危, 2：中危, 3：高危, 4：严重
NodeDesc	是	否	String	通用节点的描述

名称	必选	允许NULL	类型	描述
NodeDetail	是	否	String	节点详情
NodeId	是	否	String	节点ID
StartTime	是	否	String	开始时间
TimeLineNum	是	否	Uint64	时间线编号，同一个编号的节点属于同一个时间线

ExportInfo

日志下载任务列表

被如下接口引用：DescribeLogExports

名称	必选	允许NULL	类型	描述
CosPath	是	否	String	日志导出路径
Count	是	否	Int64	日志导出数量
CreateTime	是	否	String	日志导出创建时间
EndTime	是	否	Int64	日志导出结束时间，uinx毫秒时间戳
ExportId	是	否	String	日志导出任务ID
FileName	是	否	String	日志导出文件名
FileSize	是	否	Int64	日志文件大小
Format	是	否	String	日志导出格式
Order	是	否	String	日志导出时间排序
Query	是	否	String	日志导出查询语句
StartTime	是	否	Int64	日志导出起始时间，uinx毫秒时间戳
Status	是	否	String	日志下载状态。Processing:导出正在进行中，Complete:导出完成，Failed:导出失败，Expired:日志导出已过期（三天有效期）。

BanWhiteList

阻断白名单规则

被如下接口引用：CreateBanWhiteList、ModifyBanWhiteList

名称	必选	允许NULL	类型	描述
CreateTime	否	否	Datetime	创建白名单时间。
Id	否	否	String	白名单ID。
IsGlobal	否	是	Bool	白名单是否全局
ModifyTime	否	否	Datetime	修改白名单时间。
Quuids	否	是	Array of String	白名单所属机器列表
Remark	否	否	String	白名单别名。
SrcIp	否	否	String	阻断来源IP。
Uuid	否	是	String	白名单所属机器。

BruteAttackRule

标准阻断模式规则

被如下接口引用：ModifyBruteAttackRules

名称	必选	允许NULL	类型	描述
LoginFailTimes	是	否	Uint64	爆破事件失败次数
TimeRange	是	否	Uint64	爆破事件发生的时间范围，单位：秒

ApiKey

API密钥结果

被如下接口引用：

名称	必选	允许NULL	类型	描述
CreateTime	是	否	Uint64	创建时间(时间戳)
SecretId	是	否	String	密钥ID
Status	是	否	Uint64	状态(2:有效, 3:禁用, 4:已删除)

BaselineItemDetect

基线检测项

被如下接口引用：DescribeBaselineItemDetectList

名称	必选	允许NULL	类型	描述
DetectResult	是	是	String	检测结果,Json字符串
DetectStatus	是	是	Int64	0:未通过 1:忽略 3:通过 5:检测中
FirstTime	是	是	String	首次检测时间
FixMethod	是	是	String	修复方法
HostCount	是	是	Int64	影响服务器数
ItemDesc	是	是	String	项描述
ItemId	是	是	Int64	项Id
ItemName	是	是	String	项名称
LastTime	是	是	String	最后检测时间
Level	是	是	Int64	风险等级
NotPassedHostCount	是	是	Int64	未通过的服务器数
PassedHostCount	是	是	Int64	通过的服务器数
RuleId	是	是	Int64	所属规则ID
RuleName	是	是	String	所属规则

LicenseUnBindRsp

授权解绑信息

被如下接口引用：ModifyLicenseUnBinds

名称	必选	允许NULL	类型	描述
ErrMsg	是	否	String	失败原因
Quuid	是	否	String	QUUID 云服务器uuid,轻量服务器uuid,边缘计算 uuid

FileProtectAutoRecoverInfo

主机安全-文件防护自动恢复开关

被如下接口引用：

名称	必选	允许NULL	类型	描述
Fail	是	是	Array of Uint64	失败的防护目录ID
Offline	是	是	Array of Uint64	离线的防护目录ID
Success	是	是	Array of Uint64	响应成功的防护目录ID

ScreenInvasion

大屏入侵事件详情

被如下接口引用：DescribeScreenHostInvasion

名称	必选	允许NULL	类型	描述
Content	是	否	String	事件数据的json, 每种事件不同，【文件查杀】病毒名 VirusName、文件名 FileName、文件路径 FilePath、文件大小 FileSize、文件MD5 MD5、首次发现时间 CreateTime、最近检测时间LatestScanTime、危害描述 HarmDescribe、修复建议SuggestScheme【异常登录】来源IP SrcIp、来源地 Location、登录用户名 UserName、登录时间 LoginTime【密码破解】来源IP SrcIp、来源地 City,Country、协议 Protocol、登录用户名 UserName 、端口 Port、尝试次数 Count、首次攻击时间 CreateTime、最近攻击时间 ModifyTime【恶意请求】恶意请求域名 Url、进程ProcessName 、MD5 ProcessMd5、PID Pid、请求次数 AccessCount、最近请求时间 MergeTime、危害描述 HarmDescribe、修复建议SuggestScheme【高危命令】命中规则名 RuleName、规则类别 RuleCategory、命令内容 BashCmd、数据来源 DetectBy、登录用户 User、PID Pid、发生时间 CreateTime 、危害描述 HarmDescribe、修复建议SuggestScheme【本地提权】提权用户 UserName、父进程 ParentProcName 、父进程所属用户 ParentProcGroup、发现时间 CreateTime、危害描述 HarmDescribe、修复建议SuggestScheme【反弹shell】连接进程 ProcessName、执行命令CmdLine、父进程ParentProcName、目标主机DstIp、目标端口DstPort、发现时间 CreateTime、危害描述 HarmDescribe、修复建议SuggestScheme
CreatedTime	是	否	String	入侵时间
EventType	是	否	Uint64	事件类型：0：文件查杀，1：异常登录， 2：密码破解，3：恶意请求，4：高危命令，5：本地提权， 6：反弹shell
Id	是	否	Uint64	事件id
Level	是	否	Uint64	事件统一等级 0：提示，1：低危, 2：中危, 3：高危, 4：严重
LevelZh	是	否	String	等级中文展示
Uuid	是	否	String	主机uuid

ScreenProtection

大屏可视化攻防状态

被如下接口引用：DescribeScreenProtectionStat

名称	必选	允许NULL	类型	描述
Name	是	否	String	类型值：文件查杀，暴力破解，漏洞扫描，基线检测

名称	必选	允许NULL	类型	描述
Status	是	否	Uint64	文件查杀: 0:从未检测过，或0资产付费情况, 1:已检测，存在恶意文件, 2:已检测，未开启隔离防护, 3:已检测且已开启防护且无风险；暴力破解: 0:未开启防护（0付费资产情况）1:已开启自动阻断；漏洞扫描: 0:从未检测过，或0资产付费情况, 1:存在漏洞风险, 2:无风险；基线检测: 0:从未检测过，或0资产付费情况, 1:存在基线风险,2:无风险；

LicenseBindDetail

授权绑定详情信息

被如下接口引用：DescribeLicenseBindList

名称	必选	允许NULL	类型	描述
AgentStatus	否	否	String	云镜客户端状态,OFFLINE 离线,ONLINE 在线,UNINSTALL 未安装
IsSwitchBind	否	否	Bool	是否允许换绑,false 不允许换绑
IsUnBind	否	否	Bool	是否允许解绑,false 不允许解绑
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
MachineIp	否	否	String	机器内网IP
MachineName	否	否	String	机器别名
MachineWanIp	否	否	String	机器公网IP
Quuid	否	否	String	云服务器UUID
Tags	否	否	Array of String	标签信息
Uuid	否	否	String	云镜客户端UUID

Place

登录地信息

被如下接口引用：AddLoginWhiteList、AddLoginWhiteLists、CreateUsualLoginPlaces、DescribeLoginWhiteCombinedList、DescribeLoginWhiteList、DescribeLoginWhiteListNew、ModifyLoginWhiteInfo、ModifyLoginWhiteList、ModifyLoginWhiteRecord

名称	必选	允许NULL	类型	描述
CityId	是	否	Uint64	城市 ID。
CountryId	是	否	Uint64	国家ID，暂只支持国内：1。
Location	否	否	String	位置名称
ProvinceId	是	否	Uint64	省份 ID。

ABTestConfig

灰度项目配置

被如下接口引用：DescribeABTestConfig

名称	必选	允许NULL	类型	描述
ProjectName	是	否	String	灰度项目名称
Status	是	否	Bool	true：正在灰度，false：不在灰度

RansomDefenseRollbackTask

防勒索回滚任务

被如下接口引用：DescribeRansomDefenseRollBackTaskList

名称	必选	允许NULL	类型	描述
BackupTime	是	否	String	快照时间
CreateTime	是	否	String	操作时间
Disks	是	否	String	硬盘id列表，;分隔
Id	是	否	Uint64	任务ID
MachineName	是	否	String	主机名称
ModifyTime	是	否	String	Status!=0时为完成时间
Quuid	是	否	String	主机Quuid
RegionInfo	是	否	RegionInfo	可用区信息
Status	是	否	Uint64	回滚任务状态：0进行中，1成功，2失败
Uuid	是	否	String	主机Uuid

ProtectDirRelatedServer

防护目录关联服务器列表信息

被如下接口引用：DescribeProtectDirRelatedServer

名称	必选	允许NULL	类型	描述
Authorization	否	否	Bool	是否已经授权
AutoRestoreSwitchStatus	否	否	Uint64	自动恢复开关
Exception	否	否	Uint64	异常状态
ExceptionMessage	否	否	String	异常信息
HostIp	否	否	String	服务器IP
HostName	否	否	String	服务器名称
Id	否	否	String	唯一ID
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
MachineOs	否	否	String	服务器系统
Progress	否	否	Uint64	过渡进度
ProtectStatus	否	否	Uint64	防护状态
ProtectSwitch	否	否	Uint64	防护开关
Quuid	否	否	String	服务器唯一ID
RelateDirNum	否	否	Uint64	关联目录数

Vuls

漏洞列表数据

被如下接口引用：

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	漏洞ID
ImpactHostCount	是	否	Uint64	受影响机器数量
LastScanTime	是	否	Datetime	最后扫描时间
VulLevel	是	否	String	漏洞危害等级:HIGH：高危MIDDLE：中危LOW：低危NOTICE：提示
VulName	是	否	String	漏洞名称

VulEffectHostList

漏洞影响主机列表

被如下接口引用：DescribeVulEffectHostList

名称	必选	允许NULL	类型	描述
AliasName	否	是	String	主机别名
CloudTags	否	是	Array of Tags	云标签信息
Description	否	是	String	说明
EventId	否	是	Uint64	事件id
FirstDiscoveryTime	否	是	String	首次发现时间
FixStatusMsg	否	是	String	失败原因
HostIp	否	是	String	主机HostIp
HostVersion	否	是	Uint64	版本信息：0-基础版 1-专业版 2-旗舰版 3-普惠版
InstanceState	否	是	String	实例状态："PENDING"-创建中 "LAUNCH_FAILED"-创建失败 "RUNNING"-运行中 "STOPPED"-关机 "STARTING"-表示开机中 "STOPPING"-表示关机中 "REBOOTING"-重启中 "SHUTDOWN"-表示停止待销毁 "TERMINATING"-表示销毁中 "
IsSupportAutoFix	否	是	Uint64	是否能自动修复 0 :漏洞不可自动修复， 1：可自动修复， 2：客户端已离线， 3：主机不是旗舰版只能手动修复， 4：机型不允许 ，5：修复中 ，6：已修复， 7：检测中 9:修复失败，10:已忽略 11:漏洞只支持linux不支持Windows 12：漏洞只支持Windows不支持linux，13:修复失败但此时主机已离线，14:修复失败但此时主机不是旗舰版， 15:已手动修复
LastTime	否	是	String	最后检测时间
Level	否	是	Uint64	危害等级：1-低危；2-中危；3-高危；4-严重
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
PublicIpAddresses	否	是	String	外网ip
Quuid	否	是	String	主机Quuid
Status	否	是	Uint64	状态：0: 待处理 1:忽略 3:已修复 5:检测中 6:修复中 7: 回滚中 8:修复失败
Tags	否	是	Array of String	主机标签
Uuid	否	是	String	主机Uuid

AttackSource

攻击溯源

被如下接口引用：DescribeAttackSource

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
Edges	是	是	Array of AttackSourceEdge	攻击溯源节点路径
EventInfoParam	是	是	String	请求节点相关事件详情的参数
Nodes	是	是	Array of AttackSourceNode	攻击溯源节点描述

BashEvent

高危命令数据

被如下接口引用：DescribeBashEvents

名称	必选	允许NULL	类型	描述
BashCmd	是	否	String	执行命令
CreateTime	是	否	String	发生时间
DetectBy	是	是	Uint64	0: bash日志 1: 实时监控(雷霆版)
Exe	是	是	String	进程名称
Hostip	是	否	String	主机内网IP
Id	是	否	Uint64	数据ID
MachineName	是	否	String	主机名
ModifyTime	是	是	String	处理时间
Pid	是	是	String	进程id
Platform	是	否	Uint64	平台类型
Quuid	是	否	String	主机ID
RegexBashCmd	是	是	String	自动生成的正则表达式
RuleCategory	是	是	Uint64	规则类别 0=系统规则，1=用户规则
RuleId	是	否	Uint64	规则ID
RuleLevel	是	否	Uint64	规则等级：1-高 2-中 3-低
RuleName	是	否	String	规则名称
Status	是	否	Uint64	处理状态： 0 = 待处理 1= 已处理, 2 = 已加白， 3 = 已忽略
User	是	否	String	执行用户名
Uuid	是	否	String	云镜ID

FileTamperEvent

核心文件监控事件

被如下接口引用：DescribeFileTamperEvents

名称	必选	允许NULL	类型	描述
CreateTime	否	否	String	发生时间
Description	否	否	String	危害描述
EventCount	否	否	Uint64	事件产生次数
ExeMd5	否	否	String	进程名

名称	必选	允许NULL	类型	描述
ExeName	否	是	String	进程名称
ExePermission	否	否	String	进程权限
ExePid	否	否	Uint64	进程pid
ExeSize	否	否	Uint64	进程文件大小
ExeTime	否	否	Uint64	进程执行时长
HostIp	否	否	String	机器IP
HostName	否	否	String	机器名称
Id	否	否	Uint64	事件id
Level	否	否	Uint64	风险等级 0：无， 1: 高危， 2:中危， 3: 低危
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
MachineStatus	否	否	String	主机在线信息 ONLINE、OFFLINE
ModifyTime	否	否	String	最近发生时间
PrivateIp	否	否	String	内网ip
ProcessArgv	否	否	String	进程参数
ProcessExe	否	否	String	进程路径
Pstree	否	否	String	事件详情: json格式
Quuid	否	否	String	cvm id
Reference	否	否	String	参考链接
RuleCategory	否	否	Uint64	规则类型 0系统规则 1自定义规则
RuleId	否	否	Uint64	规则id
RuleName	否	否	String	规则名称
Status	否	否	Uint64	处理状态 0 -- 待处理 1 -- 已加白 2 -- 已删除 3 - 已忽略 4-已手动处理
Suggestion	否	否	String	修护建议
Target	否	否	String	目标文件路径
TargetCreatTime	否	是	String	目标文件创建时间
TargetModifyTime	否	是	String	目标文件更新时间
TargetName	否	否	String	文件名称
TargetPermission	否	否	String	目标文件权限
TargetSize	否	否	Uint64	目标文件大小
Type	否	否	Uint64	事件类型/动作 0 -- 告警
UserGroup	否	否	String	用户组
UserName	否	否	String	用户名
Uuid	否	否	String	主机uuid

VulDefenceEventDetail

漏洞详细信息

被如下接口引用：DescribeDefenceEventDetail

名称	必选	允许NULL	类型	描述
Alias	否	否	String	主机名
City	否	否	String	攻击源ip地址所在城市
Count	否	否	Int64	事件发生次数
CreateTime	否	否	String	创建事件时间
CveId	否	否	String	cve编号
Description	否	否	String	漏洞描述信息
EventDetail	否	否	String	漏洞ID相关的事件详情(json array格式 rasp特有)
EventType	否	否	Uint64	0: 尝试攻击(WeDetect) 1:尝试攻击成功(WeDetect) 2:rasp防御事件
ExceptionPstree	否	否	String	主机失陷事件进程树(json格式 WeDetect特有)
Fix	否	否	String	修复建议
Id	否	否	Int64	漏洞事件id
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
MachineStatus	否	否	String	ONLINE OFFLINE
MainClass	否	否	String	关联进程主类名
MergeTime	否	否	String	更新事件时间
NetworkPayload	否	否	String	攻击payload
Pid	否	否	Int64	关联进程pid
PrivateIp	否	否	String	内网ip
PublicIp	否	否	String	公网ip
Quuid	否	否	String	主机quuid
SourceIp	否	否	String	攻击源ip
SourcePort	否	是	Array of Uint64	攻击源端口
StackTrace	否	否	String	堆栈信息(rasp特有)
Status	否	否	Int64	状态 0: 待处理 1:已防御 2:已处理 3: 已忽略 4: 已删除
VulName	否	否	String	漏洞名称

AssetDiskPartitionInfo

资产管理磁盘分区信息

被如下接口引用：DescribeAssetDiskList、DescribeAssetMachineDetail

名称	必选	允许NULL	类型	描述
Name	是	否	String	分区名
Path	是	否	String	挂载目录
Percent	是	否	Float	分区使用率
Size	是	否	Uint64	分区大小：单位G
Type	是	否	String	文件系统类型

名称	必选	允许NULL	类型	描述
Used	是	否	Uint64	已使用空间：单位G

Strategy

基线安全用户策略信息

被如下接口引用：DescribeBaselineStrategyList

名称	必选	允许NULL	类型	描述
CategoryIds	是	是	String	基线id
Enabled	是	是	Uint64	是否可用
HostCount	是	是	Uint64	主机数量
IsDefault	是	是	Uint64	是否默认策略
PassRate	是	是	Uint64	通过率
RuleCount	是	是	Uint64	基线检测项总数
ScanAt	是	是	String	扫描时间
ScanCycle	是	是	Uint64	扫描周期
StrategyId	是	是	Uint64	策略id
StrategyName	是	是	String	策略名

PortInfo

容器安全端口信息列表

被如下接口引用：

名称	必选	允许NULL	类型	描述
ContainerName	是	否	String	容器名
ContainerPID	是	否	Uint64	容器内PID
ContainerPort	是	否	Uint64	容器端口
HostID	是	否	String	主机id
HostIP	是	否	String	主机ip
ListenContainer	是	否	String	容器内监听地址
ListenHost	是	否	String	容器外监听地址
ProcessName	是	否	String	进程名
PublicIP	是	否	String	对外ip
PublicPort	是	否	Uint64	主机端口
RunAs	是	否	String	运行账号
Type	是	否	String	类型

IgnoreRuleEffectHostInfo

忽略检测项影响主机信息

被如下接口引用：DescribeIgnoreRuleEffectHostList

名称	必选	允许NULL	类型	描述
EventId	是	是	Uint64	事件id
HostName	是	是	String	主机名称
LastScanTime	是	是	String	最后检测时间
Level	是	是	Uint64	危害等级：1-低位，2-中危，3-高危，4-严重
Quuid	是	是	String	主机quuid
Status	是	是	Uint64	状态：0-未通过，1-忽略，3-已通过，5-检测中
TagList	是	是	Array of String	主机标签数组

ScreenNameValue

【云安全预警】大屏可视化数据Name Value 数据

被如下接口引用：DescribeScreenEventsCnt、DescribeScreenGeneralStat、DescribeScreenRiskAssetsTop

名称	必选	允许NULL	类型	描述
Name	是	否	String	统计类型 不同接口对应不同的内容
Value	是	否	Uint64	统计数量

AssetAppProcessInfo

软件应用关联进程信息

被如下接口引用：DescribeAssetAppProcessList、DescribeAssetJarInfo、DescribeAssetWebServiceProcessList

名称	必选	允许NULL	类型	描述
Name	是	否	String	名称
Path	是	否	String	路径
StartTime	是	否	String	启动时间
Status	是	否	String	进程状态
User	是	否	String	用户
Version	是	否	String	进程版本

WebHookHostLabel

企微机器人主机范围

被如下接口引用：DescribeWebHookRule、DescribeWebHookRules、ModifyWebHookRule

名称	必选	允许NULL	类型	描述
Type	是	否	Int64	主机范围[1:所属项目|2:腾讯云标签|3:主机安全标签|4:自选]空数组为全部
Values	是	否	Array of String	主机项目或标签内容

Component

组件列表数据。

被如下接口引用：DescribeComponents

名称	必选	允许NULL	类型	描述
ComponentName	是	否	String	组件名称。
ComponentType	是	否	String	组件类型。 - SYSTEM：系统组件 - WEB：Web组件
ComponentVersion	是	否	String	组件版本号。
Id	是	否	Uint64	唯一ID。
MachineIp	是	否	String	主机内网IP。
MachineName	是	否	String	主机名。
ModifyTime	是	否	Datetime	组件检测更新时间。
Uuid	是	否	String	云镜客户端唯一Uuid。

OpenPortStatistics

端口统计列表

被如下接口引用：DescribeOpenPortStatistics

名称	必选	允许NULL	类型	描述
MachineNum	是	否	Uint64	主机数量
Port	是	否	Uint64	端口号

LicenseDetail

授权订单列表对象

被如下接口引用：DescribeLicenseList

名称	必选	允许NULL	类型	描述
Alias	是	否	String	资源别名
AutoRenewFlag	是	否	Uint64	0 初始化,1 自动续费,2 不自动续费
BuyTime	是	否	String	购买时间
Deadline	是	否	String	截止日期
LicenseCnt	是	否	Uint64	总授权数
LicenseId	是	否	Uint64	授权ID
LicenseStatus	是	是	Uint64	授权状态 0 未使用,1 部分使用, 2 已用完, 3 不可用
LicenseType	是	否	Uint64	授权类型,0 专业版-按量计费, 1专业版-包年包月 , 2 旗舰版-包年包月
OrderStatus	是	否	Uint64	订单状态 1 正常 2隔离, 3销毁
ProjectId	是	否	Uint64	项目ID
ResourceId	是	否	String	订单资源ID
SourceType	是	否	Uint64	是否试用订单.
Tags	是	是	Array of Tags	平台标签
TaskId	是	否	Uint64	任务ID ,默认0 ,查询绑定进度用

名称	必选	允许NULL	类型	描述
UsedLicenseCnt	是	否	Uint64	已使用授权数

BashRule

高危命令规则

被如下接口引用：DescribeBashRules

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建时间
DealOldEvents	是	是	Uint64	是否处理之前的事件 0: 不处理 1:处理
Decription	是	否	String	规则描述
Hostip	是	否	String	主机IP
Id	是	否	Uint64	规则ID
IsGlobal	是	否	Uint64	是否全局规则
Level	是	否	Uint64	危险等级(0 ：无 1: 高危 2:中危 3: 低危)
ModifyTime	是	否	String	修改时间
Name	是	否	String	规则名称
Operator	是	否	String	操作人
Rule	是	否	String	正则表达式
Status	是	否	Uint64	状态 (0: 有效 1: 无效)
Uuid	是	否	String	客户端ID
Uuids	是	是	Array of String	生效服务器的uuid数组
White	是	是	Uint64	0=黑名单 1=白名单

ImpactedHost

受影响主机信息

被如下接口引用：DescribeImpactedHosts

名称	必选	允许NULL	类型	描述
Description	是	否	String	漏洞描述。
Id	是	否	Uint64	漏洞ID。
IsProVersion	是	否	Bool	是否为专业版。
LastScanTime	是	否	Datetime	最后检测时间。
MachineIp	是	否	String	主机IP。
MachineName	是	否	String	主机名称。
Uuid	是	否	String	云镜客户端唯一标识UUID。
VulId	是	否	Uint64	漏洞种类ID。
VulStatus	是	否	String	漏洞状态。 - UN_OPERATED ：待处理 - SCANING : 扫描中 - FIXED : 已修复

PushTaskResult

快捷防护-下发检测，扫描结果

被如下接口引用：CreateQuickProtectSetting

名称	必选	允许NULL	类型	描述
FailureReason	是	否	String	下发失败原因
IsSuccess	是	否	Bool	是否下发成功
TaskId	是	否	Uint64	对应任务Id
TaskType	是	否	String	任务种类：Vul-检测漏洞，Malware-文件查杀，Baseline-基线检测，AutoBan-自动阻断

MachineSimple

主机列表穿梭框

被如下接口引用：DescribeMachinesSimple

名称	必选	允许NULL	类型	描述
CloudTags	否	是	Array of Tags	云标签信息
InstanceId	否	是	String	实例ID
InstanceState	否	否	String	实例状态 TERMINATED_PRO_VERSION 已销毁
IsProVersion	否	否	Bool	是否是专业版。 - true： 是 - false：否
KernelVersion	否	否	String	内核版本
LicenseOrder	否	是	LicenseOrder	授权订单对象
MachineIp	否	否	String	主机IP。
MachineName	否	否	String	主机名称。
MachineOs	否	否	String	主机系统。
MachineType	否	否	String	机器所属专区类型 CVM 云服务器, BM 黑石, ECM 边缘计算, LH 轻量应用服务器 ,Other 混合云专区
MachineWanIp	否	否	String	主机外网IP。
PayMode	否	否	String	主机状态。 - POSTPAY: 表示后付费，即按量计费 - PREPAY: 表示预付费，即包年包月
ProjectId	否	否	Int64	项目ID
ProtectType	否	否	String	防护版本 BASIC_VERSION 基础版， PRO_VERSION 专业版，Flagship 旗舰版，GENERAL_DISCOUNT 普惠版.
Quuid	否	否	String	CVM或BM机器唯一Uuid。
RegionInfo	否	否	RegionInfo	地域信息
Tag	否	否	Array of MachineTag	标签信息
Uuid	否	否	String	云镜客户端唯一Uuid，若客户端长时间不在线将返回空字符。

AssetUserKeyInfo

资产管理账号key详情

被如下接口引用：DescribeAssetUserInfo、DescribeAssetUserKeyList

名称	必选	允许NULL	类型	描述
Comment	是	否	String	公钥备注
EncryptType	是	否	String	加密方式
Value	是	否	String	公钥值

ZoneInfo

可用区信息

被如下接口引用：DescribeBanRegions

名称	必选	允许NULL	类型	描述
ZoneName	是	否	String	可用区名称

HostLoginList

登录审计列表实体

被如下接口引用：DescribeHostLoginList

名称	必选	允许NULL	类型	描述
City	否	是	Uint64	城市id
Country	否	是	Uint64	国家id
Desc	否	是	String	高危信息说明：ABROAD - 海外IP；XTI - 威胁情报
Id	否	否	Uint64	记录Id
IsRiskArea	否	是	Uint64	是否命中异地登录异常 1表示命中此类异常, 0表示未命中
IsRiskSrcIp	否	是	Uint64	是否命中异常IP异常 1表示命中此类异常, 0表示未命中
IsRiskTime	否	是	Uint64	是否命中异常时间异常 1表示命中此类异常, 0表示未命中
IsRiskUser	否	是	Uint64	是否命中异常用户异常 1表示命中此类异常, 0表示未命中
Location	否	是	String	位置名称
LoginTime	否	是	String	登录时间
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	是	String	主机ip
MachineName	否	是	String	主机名
ModifyTime	否	是	String	修改时间
Province	否	是	Uint64	省份id
Quuid	否	是	String	主机quuid
RiskLevel	否	是	Uint64	危险等级：0 高危1 可疑
SrcIp	否	是	String	来源ip
Status	否	否	Uint64	1:正常登录；2异地登录； 5已加白； 14：已处理；15：已忽略。
UserName	否	是	String	用户名
Uuid	否	是	String	Uuid串

MalWareList

木马列表集合

被如下接口引用：DescribeMalWareList

名称	必选	允许NULL	类型	描述
Alias	否	否	String	主机别名
CheckPlatform	否	否	String	'木马检测平台用,分割 1云查杀引擎、2TAV、3binaryAi、4异常行为、5威胁情报
CreateTime	否	否	String	创建时间
FileCreateTime	否	是	String	首次运行时间
FileExists	否	否	Uint64	木马文件是否存在 0:不存在，1:存在
FileModifierTime	否	是	String	最近运行时间
FilePath	否	否	String	路径
HostIp	否	否	String	服务器ip
Id	否	是	Uint64	唯一ID
LatestScanTime	否	否	String	最近扫描时间
Level	否	否	Uint64	风险等级 0未知、1低、2中、3高、4严重
MD5	否	否	String	木马样本md5
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
ProcessExists	否	否	Uint64	木马进程是否存在 0:不存在，1:存在
Quuid	否	否	String	cvm quuid
Status	否	否	Uint64	状态；4-:待处理，5-已信任，6-已隔离，8-文件已删除, 14:已处理
Tags	否	是	Array of String	特性标签，已废弃字段，不会再返回标签，详情中才会返回标签信息
Uuid	否	否	String	唯一UUID
VirusName	否	否	String	描述

Machine

主机列表

被如下接口引用：DescribeMachineList、DescribeMachines

名称	必选	允许NULL	类型	描述
BaselineNum	否	否	Int64	基线风险数。
CloudTags	否	是	Array of Tags	云标签信息
CyberAttackNum	否	否	Int64	网络风险数。
HasAssetScan	否	否	Uint64	是否有资产扫描接口，0无，1有
InstanceId	否	否	String	实例ID
InstanceState	否	否	String	实例状态 TERMINATED_PRO_VERSION 已销毁
InvasionNum	否	否	Int64	入侵事件数
IpList	否	是	String	主机ip列表

名称	必选	允许NULL	类型	描述
IsAddedOnTheFifteen	否	是	Uint64	是否15天内新增的主机 0：非15天内新增的主机，1：15天内增加的主机
IsProVersion	否	否	Bool	是否是专业版。 - true： 是 - false：否
KernelVersion	否	否	String	内核版本
LicenseStatus	否	否	Uint64	防篡改 授权状态 1 授权 0 未授权
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	主机IP。
MachineName	否	否	String	主机名称。
MachineOs	否	否	String	主机系统。
MachineStatus	否	否	String	主机状态。 - OFFLINE: 离线 - ONLINE: 在线 - SHUTDOWN: 已关机 - UNINSTALLED: 未防护
MachineType	否	否	String	机器所属专区类型 CVM 云服务器, BM 黑石, ECM 边缘计算, LH 轻量应用服务器 ,Other 混合云专区
MachineWanIp	否	否	String	主机外网IP。
MalwareNum	否	否	Int64	木马数。
PayMode	否	否	String	主机状态。 - POSTPAY: 表示后付费，即按量计费 - PREPAY: 表示预付费，即包年包月
ProjectId	否	否	Int64	项目ID
ProtectType	否	否	String	防护版本：BASIC_VERSION 基础版， PRO_VERSION 专业版，Flagship 旗舰版，GENERAL_DISCOUNT 普惠版
Quuid	否	否	String	CVM或BM机器唯一Uuid。
RegionInfo	否	否	RegionInfo	地域信息
Remark	是	是	String	备注信息
SecurityStatus	否	否	String	风险状态。 - SAFE：安全 - RISK：风险 - UNKNOWN：未知
Tag	否	否	Array of MachineTag	标签信息
Uuid	否	否	String	云镜客户端唯一Uuid，若客户端长时间不在线将返回空字符。
VpcId	否	是	String	所属网络
VulNum	否	否	Int64	漏洞数。

DuplicateHosts

批量添加白名单：重复情况重复列表实体

被如下接口引用：AddLoginWhiteLists、CreateBanWhiteList

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	Id
Quuid	是	是	String	Quuid
Uuid	是	是	String	Uuid

ScanTaskDetails

扫描任务详情列表信息

被如下接口引用：DescribeScanTaskDetails

名称	必选	允许NULL	类型	描述
Description	否	否	String	描述
FailType	否	否	Uint64	失败详情
HostIp	否	否	String	服务器IP
HostName	否	否	String	服务器名称
Id	否	否	Uint64	id唯一
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineWanIp	否	否	String	外网ip
OsName	否	否	String	操作系统
Quuid	否	否	String	唯一Quuid
RiskNum	否	否	Uint64	风险数量
ScanBeginTime	否	否	String	扫描开始时间
ScanEndTime	否	否	String	扫描结束时间
Status	否	否	String	状态码
Uuid	否	否	String	唯一Uuid

ImageInfo

容器安全镜像列表

被如下接口引用：

名称	必选	允许NULL	类型	描述
AgentError	是	否	String	agent镜像扫描错误
BuildHistory	是	否	String	构建历史
ContainerCnt	是	否	Uint64	关联容器个数
CreateTime	是	否	String	创建时间
HostCnt	是	否	Uint64	关联主机数
ImageID	是	否	String	镜像id
ImageName	是	否	String	镜像名称
IsTrustImage	是	否	Bool	是否可信镜像
OsName	是	否	String	镜像系统
RiskCnt	是	否	Uint64	风险行为数
ScanError	是	否	String	后端镜像扫描错误
ScanStatus	是	否	String	扫描状态
ScanTime	是	否	String	最近扫描时间
SensitiveInfoCnt	是	否	Uint64	敏感信息数
Size	是	否	Uint64	镜像大小

名称	必选	允许NULL	类型	描述
VirusCnt	是	否	Uint64	病毒木马数
VulCnt	是	否	Uint64	漏洞数

VersionWhiteConfig

授权版本白名单配置信息

被如下接口引用：DescribeLicenseWhiteConfig

名称	必选	允许NULL	类型	描述
Deadline	是	否	Uint64	到期天数
IsApplyFor	是	否	Bool	是否可申请
LicenseNum	是	否	Uint64	授权数量
SourceType	是	否	Uint64	类型

RansomDefenseStrategyDetail

主机列表查询接口相应数据HostList的TagList节点

被如下接口引用：DescribeRansomDefenseStrategyDetail

名称	必选	允许NULL	类型	描述
BackupType	是	是	Uint64	备份模式： 0按周，1按天
CreateTime	是	是	String	创建时间
Description	是	是	String	策略备注
EventCount	是	是	Uint64	策略关联事件数
ExcludeDir	是	是	String	包含目录，用;分隔
Hour	是	否	String	备份执行时间点(0-23): 11:00;12:00
Id	是	否	Int64	策略id
IncludeDir	是	是	String	包含目录，用;分隔
IsAll	是	否	Uint64	是否对所有主机生效
MachineCount	是	是	Uint64	绑定机器数
ModifyTime	是	是	String	最近修改时间
Name	是	否	String	策略名称
SaveDay	是	否	Uint64	保存天数，0永久保存
Status	是	否	Uint64	开启状态：0关闭，1开启
Uin	是	是	String	操作uin
Weekday	是	是	String	备份星期天数（1-7）：1;2;3;4

VulDefenceEvent

漏洞详细信息

被如下接口引用：DescribeVulDefenceEvent

名称	必选	允许NULL	类型	描述
Alias	否	否	String	主机名
City	否	否	String	攻击源ip地址所在城市
Count	否	否	Int64	事件发生次数
CreateTime	否	否	String	创建事件时间
CveId	否	否	String	cve编号
EventType	否	否	Uint64	0: 尝试攻击(WeDetect) 1:尝试攻击成功(WeDetect) 2:rasp防御事件
FixType	否	否	Int64	0 不支持修复，1 支持修复
Id	否	否	Int64	漏洞事件id
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
MergeTime	否	否	String	更新事件时间
PrivateIp	否	否	String	内网ip
PublicIp	否	否	String	公网ip
Quuid	否	否	String	主机quuid
SourceIp	否	否	String	攻击源ip
SourcePort	否	否	Array of Uint64	攻击源端口
Status	否	否	Int64	状态 0: 待处理 1:已防御 2:已处理 3: 已忽略 4: 已删除
UpgradeType	否	否	Int64	0 专业版,1 旗舰版,2 LH普惠版（仅限LH使用）,3 CVM普惠版（仅限CVM使用）
Uuid	否	否	String	主机uuid
VulId	否	否	Uint64	漏洞ID
VulName	否	否	String	漏洞名称

VulDefencePluginStatus

主机漏洞防御插件信息

被如下接口引用：DescribeVulDefencePluginStatus

名称	必选	允许NULL	类型	描述
Alias	是	否	String	主机别名
CreateTime	是	否	String	创建时间
Exception	是	否	Int64	插件状态：0 正常，1 异常
ModifyTime	是	否	String	最后跟新时间
PrivateIp	是	否	String	内网ip
PublicIp	是	否	String	公网ip
Quuid	是	否	String	主机quuid

SecurityTrend

安全趋势统计数据。

被如下接口引用：DescribeEventTrend、DescribeSecurityTrends

名称	必选	允许NULL	类型	描述
Date	是	否	Date	事件时间。
EventNum	是	否	Uint64	事件数量。

WebHookEventKv

企微机器人事件类型

被如下接口引用：DescribeWebHookRule、DescribeWebHookRules、ModifyWebHookRule

名称	必选	允许NULL	类型	描述
ControlBit	是	否	String	事件内容
Type	是	否	Int64	事件类型

CanNotSeparateInfo

不可隔离木马的机器信息

被如下接口引用：DescribeCanNotSeparateMachine

名称	必选	允许NULL	类型	描述
Alias	是	否	String	主机名
PrivateIp	是	否	String	内网ip
PublicIp	是	否	String	外网ip
Quuid	是	否	String	主机quuid
Reason	是	否	Uint64	隔离失败原因 1:agent离线
Uuid	是	否	String	主机uuid

NetAttackEventInfo

被如下接口引用：DescribeAttackEventInfo

名称	必选	允许NULL	类型	描述
AbnormalAction	否	是	String	异常行为
AttackLevel	否	是	Uint64	漏洞攻击热度
CVEId	否	是	String	漏洞CVE编号
Count	否	是	Uint64	攻击次数
DstPort	否	是	Uint64	目标端口
HostOpProcessTree	否	是	String	进程树,需要用base64 解码
HostOpType	否	是	Uint64	0:无失陷行为 1: rce(命令执行) 2: dnslog 3: writefile
Id	否	是	Uint64	事件id
Location	否	是	String	攻击源地
MachineExtraInfo	否	是	MachineExtraInfo	主机额外信息
MergeTime	否	是	String	攻击发生时间

名称	必选	允许NULL	类型	描述
NetPayload	否	是	String	攻击数据包
PayVersion	否	是	Uint64	机器付费版本，0 基础版，1专业版，2旗舰版，3普惠版
Quuid	否	是	String	cvm uuid
SrcIP	否	是	String	攻击源ip
Status	否	是	Uint64	处理状态，0 待处理 1 已处理 2 已加白 3 已忽略 4 已删除 5: 已开启防御
SvcPs	否	是	String	服务进程 base64
Type	否	是	Uint64	0: 尝试攻击 1:攻击成功
Uuid	否	是	String	主机uuid
VulDefenceStatus	否	是	Uint64	漏洞防御状态，0关闭，1开启
VulId	否	是	Uint64	漏洞id
VulName	否	是	String	漏洞名称
VulSupportDefense	否	是	Uint64	漏洞是否支持防御，0:不支持 1:支持

HostInfo

添加登录审计白名单的主机信息实体

被如下接口引用：AddLoginWhiteLists、ModifyLoginWhiteRecord

名称	必选	允许NULL	类型	描述
Quuid	是	否	String	Quuid
Uuid	是	否	String	Uuid

RecordInfo

客户端异常信息结构

被如下接口引用：DescribeClientException

名称	必选	允许NULL	类型	描述
HostIP	是	否	String	主机ip
InstanceID	是	否	String	主机实例id
OfflineTime	是	否	String	客户端离线时间
UninstallCmd	是	否	String	客户端卸载调用链
UninstallTime	是	否	String	客户端卸载时间
Uuid	是	否	String	客户端uuid

LoginWhiteCombinedInfo

异地登录合并后白名单

被如下接口引用：DescribeLoginWhiteCombinedList

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建时间
Desc	是	否	String	仅在单台服务器时，返回服务器名称
EndTime	是	否	String	结束时间
Id	是	否	Uint64	白名单ID
IsGlobal	是	否	Uint64	是否对全局生效, 1：全局有效 0: 对指定主机列表生效'
Locale	是	否	String	地域字符串
Locations	是	否	String	登陆地
ModifyTime	是	否	String	最近修改时间
Name	是	否	String	白名单名字：IsLocal=1时固定为：全部服务器；单台机器时为机器内网IP，多台服务器时为服务器数量，如：11台
Places	是	是	Array of Place	白名单地域
Remark	是	否	String	备注
SrcIp	是	否	String	白名单IP（多个IP逗号隔开）
StartTime	是	否	String	开始时间
UserName	是	否	String	白名单用户（多个用户逗号隔开）
Uuid	是	否	String	服务器Uuid

AssetFilters

容器安全 描述键值对过滤器，用于条件过滤查询。例如过滤ID、名称、状态等 若存在多个Filter时，Filter间的关系为逻辑与（AND）关系。 若同一个Filter存在多个Values，同一Filter下Values间的关系为逻辑或（OR）关系。

被如下接口引用：DescribeAssetAppList、DescribeAssetCoreModuleList、DescribeAssetDatabaseList、DescribeAssetEnvList、DescribeAssetInitServiceList、DescribeAssetJarList、DescribeAssetPlanTaskList、DescribeAssetWebServiceInfoList、DescribeLoginWhiteHostList、DescribeMachineList、DescribeProtectDirList、DescribeWebPageEventList、ExportAssetAppList、ExportAssetCoreModuleList、ExportAssetDatabaseList、ExportAssetEnvList、ExportAssetInitServiceList、ExportAssetJarList、ExportAssetPlanTaskList、ExportAssetWebServiceInfoList、ExportProtectDirList、ExportWebPageEventList

名称	必选	允许NULL	类型	描述
ExactMatch	否	否	Bool	是否模糊查询
Name	是	否	String	过滤键的名称。
Values	是	否	Array of String	一个或者多个过滤值。

RansomDefenseEvent

防勒索诱饵篡改事件

被如下接口引用：DescribeRansomDefenseEventsList

名称	必选	允许NULL	类型	描述
BaitFilePath	是	否	String	被篡改文件路径
CreateTime	是	否	String	事件发送时间
FileMd5	是	否	String	恶意文件md5
FilePath	是	否	String	恶意文件路径

名称	必选	允许NULL	类型	描述
FileSize	是	否	Uint64	恶意文件大小
HostIp	是	否	String	主机外网ip
HostName	是	否	String	主机名称
Id	是	否	Uint64	事件id
InstanceId	是	否	String	cvm 实例id
ModifyTime	是	否	String	事件修改事件
Pid	是	否	Uint64	恶意进程id
PidParam	是	否	String	恶意进程参数
ProcessStartTime	是	否	String	进程启动时间
PsTree	是	否	String	进程树 base64 json
Quuid	是	否	String	cvm uuid
SnapshotNum	是	否	Uint64	主机拥有快照备份数
Status	是	否	Uint64	事件状态 0待处理，1已处理，2已信任，3处理中，4已恢复备份
StrategyId	是	否	Uint64	策略id
StrategyName	是	否	String	策略名称
Type	是	否	Uint64	事件类型：0加密勒索，1文件篡改
Uuid	是	否	String	主机uuid
WanIp	是	否	String	主机内网ip

AssetJarBaseInfo

资产管理jar包列表

被如下接口引用：DescribeAssetJarList、DescribeAssetWebFrameJarList

名称	必选	允许NULL	类型	描述
FirstTime	否	否	String	首次采集时间
Id	否	否	String	Jar包ID
IsNew	否	否	Int64	是否新增[0:否|1:是]
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	服务器IP
MachineName	否	否	String	服务器名称
MachineWanIp	否	否	String	服务器外网IP
Md5	否	否	String	Jar包Md5
Name	否	否	String	名称
OsInfo	否	否	String	操作系统
Path	否	否	String	路径
Quuid	否	否	String	主机Quuid
Status	否	否	Uint64	是否可执行：0未知，1是，2否

名称	必选	允许NULL	类型	描述
Type	否	否	Int64	类型：1应用程序，2系统类库，3Web服务自带库，8:其他，
UpdateTime	否	是	String	数据更新时间
Uuid	否	否	String	主机uuid
Version	否	否	String	版本

RegionInfo

地域信息

被如下接口引用：DescribeMachineList、DescribeMachineRegions、DescribeMachines、DescribeMachinesSimple、DescribeRansomDefenseMachineList、DescribeRansomDefenseRollBackTaskList、DescribeRansomDefenseStrategyMachines

名称	必选	允许NULL	类型	描述
Region	是	否	String	地域标志，如 ap-guangzhou，ap-shanghai，ap-beijing
RegionCode	是	否	String	地域代码，如 gz，sh，bj
RegionId	是	否	Uint64	地域ID
RegionName	是	否	String	地域中文名，如华南地区（广州），华东地区（上海金融），华北地区（北京）
RegionNameEn	是	否	String	地域英文名

BaselineItemInfo

基线信息

被如下接口引用：DescribeBaselineItemIgnoreList、DescribeBaselineItemInfo、DescribeIgnoreHostAndItemConfig

名称	必选	允许NULL	类型	描述
FixMethod	是	否	String	检测项的修复方法
ItemDesc	是	否	String	检测项描述
ItemId	是	否	Int64	基线检测项ID
ItemName	是	否	String	检测项名字
Level	是	否	Int64	危险等级
RelatedCustomRuleInfo	是	是	Array of BaselineCustomRuleIdName	被引自定义规则信息
RuleId	是	是	Uint64	检测项所属规则的ID
RuleName	是	否	String	检测项所属规则名字
SysRuleId	是	是	Int64	系统规则ID

FileTamperRuleDetail

核心文件监控规则详情

被如下接口引用：DescribeFileTamperEventRuleInfo、DescribeFileTamperRuleInfo

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建时间
Id	是	否	Uint64	规则id

名称	必选	允许NULL	类型	描述
IsGlobal	是	否	Uint64	是否全局规则(默认否) 0：否 ，1：是
Level	是	否	Uint64	风险等级 0：无， 1: 高危， 2:中危， 3: 低危
ModifyTime	是	否	String	更新时间
Name	是	是	String	规则名称
Rule	是	否	Array of FileTamperRule	规则
Status	是	否	Uint64	状态 0: 启用 1: 已关闭
UuidTotalCount	是	否	Uint64	生效主机的总数
Uuids	是	是	Array of String	生效主机uuid,空表示全部主机，通过参数可控制返回的条数

EmergencyResponseInfo

专家服务-应急响应信息

被如下接口引用：DescribeEmergencyResponseList

名称	必选	允许NULL	类型	描述
EndTime	是	否	String	服务结束时间
HostNum	是	否	Uint64	主机个数
ReportPath	是	否	String	报告下载地址
StartTime	是	否	String	服务开始时间
Status	是	否	Uint64	服务状态 0未启动，·响应中，2响应完成
TaskId	是	否	String	任务id

RansomDefenseStrategyMachineInfo

防勒索机器硬盘配置

被如下接口引用：CreateRansomDefenseStrategy

名称	必选	允许NULL	类型	描述
DiskInfo	否	是	String	指定硬盘列表，为空时表示所有硬盘：disk_id1|disk_name1;disk_id2|disk_name2
Uuid	是	否	String	主机uuid

LoginWhiteDimension

异地登录合并后白名单

被如下接口引用：

名称	必选	允许NULL	类型	描述
EndTime	否	否	String	结束时间
Locale	否	否	String	地域字符串
Places	否	否	Array of Place	白名单地域
Remark	否	否	String	备注

名称	必选	允许NULL	类型	描述
SrcIp	否	否	String	白名单IP（多个IP逗号隔开）
StartTime	否	否	String	开始时间
UserName	否	否	String	白名单用户（多个用户逗号隔开）

AssetEnvBaseInfo

资产管理环境变量列表

被如下接口引用：DescribeAssetEnvList

名称	必选	允许NULL	类型	描述
FirstTime	否	否	String	首次采集时间
IsNew	否	否	Int64	是否新增[0:否|1:是]
MachineExtraInfo	否	是	MachineExtraInfo	附加信息
MachineIp	否	否	String	服务器IP
MachineName	否	否	String	服务器名称
MachineWanIp	否	否	String	服务器外网IP
Name	否	否	String	名称
OsInfo	否	否	String	操作系统
Quuid	否	否	String	主机Quuid
Type	否	否	Uint64	类型：0:用户变量1:系统变量
UpdateTime	否	是	String	数据更新时间
User	否	否	String	启动用户
Uuid	否	否	String	主机uuid
Value	否	否	String	环境变量值

ResponseList

隔离木马接口中成功或失败返回的machines list

被如下接口引用：

名称	必选	允许NULL	类型	描述
FilePath	是	否	String	文件路径
MachineIp	是	否	String	主机ip

WeeklyReportBruteAttack

专业周报密码破解数据。

被如下接口引用：DescribeWeeklyReportBruteAttacks

名称	必选	允许NULL	类型	描述
AttackTime	是	否	Datetime	攻击时间。

名称	必选	允许NULL	类型	描述
Count	是	否	Uint64	尝试次数。
MachineIp	是	否	String	主机IP。
SrcIp	是	否	String	源IP。
Username	是	否	String	被破解用户名。

ProVersionMachine

需要开通专业版机器信息。

被如下接口引用：InquiryPriceOpenProVersionPrepaid、OpenProVersionPrepaid

名称	必选	允许NULL	类型	描述
MachineRegion	是	否	String	主机所在地域。如：ap-guangzhou、ap-beijing
MachineType	是	否	String	主机类型。 - CVM: 云服务器 - BM: 黑石物理机 - ECM: 边缘计算服务器 - LH: 轻量应用服务器 - Other: 混合云机器
Quuid	是	否	String	主机唯一标识Uuid数组。黑石的InstanceId，CVM的Uuid ,边缘计算的Uuid，轻量应用服务器的Uuid ,混合云机器的Quuid 。 当前参数最大长度限制20

错误码

最近更新时间: 2024-09-03 18:50:09

功能说明

如果返回结果中存在 Error 字段，则表示调用 API 接口失败。例如：

```
{
"Response": {
"Error": {
"Code": "AuthFailure.SignatureFailure",
"Message": "The provided credentials could not be validated. Please check your signature is correct."
},
"RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
}
}
```

Error 中的 Code 表示错误码，Message 表示该错误的具体信息。

错误码列表

公共错误码

错误码	说明
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）。
AuthFailure.MFAFailure	MFA 错误。
AuthFailure.SecretIdNotFound	密钥不存在。 请在控制台检查密钥是否已被删除或者禁用，如状态正常，请检查密钥是否填写正确，注意前后不得有空格。
AuthFailure.SignatureExpire	签名过期。Timestamp 和服务器时间相差不得超过五分钟，请检查本地时间是否和标准时间同步。
AuthFailure.SignatureFailure	签名错误。 签名计算错误，请对照调用方式中的接口鉴权文档检查签名计算过程。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未 CAM 授权。
DryRunOperation	DryRun 操作，代表请求将会是成功的，只是多传了 DryRun 参数。
FailedOperation	操作失败。
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。

错误码	说明
UnknownParameter	未知参数错误。
UnsupportedOperation	操作不支持。
UnsupportedProtocol	http(s)请求协议错误，只支持 GET 和 POST 请求。
UnsupportedRegion	接口不支持所传地域。

业务错误码

错误码	说明
LimitExceeded	
InternalError.MainDBFail	
InvalidParameter.IpNoValid	
FailedOperation.CreateProcessTask	
OperationDenied	
UnknownParameter	
InvalidParameter	
FailedOperation.RescanVulProcessInUse	
InvalidParameter.NameHasRepetition	
FailedOperation.OpenPortTaskNotFound	
FailedOperation.InquiryPrice	
UnsupportedOperation	
FailedOperation.SingleSeparate	
ResourceUnavailable	
InvalidParameterValue.TagNameLengthLimit	
InvalidParameter.InvalidFormat	
InvalidParameter.RuleHostDuplicateErr	
FailedOperation.CloseProVersion	
ResourceNotFound.MachineNotFound	
FailedOperation.AgentOffline	
InvalidParameter.DateRange	
FailedOperation.APIServerFail	
InvalidParameter.RuleHostipErr	
InvalidParameterValue	
AuthFailure.UnauthorizedOperation	
InvalidParameter.PortNoValid	
MissingParameter	
FailedOperation.PartSeparate	
FailedOperation.LicenseExceeded	
FailedOperation.OpenProVersion	

错误码	说明
ResourceInUse	
FailedOperation.ProtectStartFail	
FailedOperation.CreateOpenPortTask	
FailedOperation.NoProfessionHost	
ResourceInsufficient	
FailedOperation.TooManyStrategy	
FailedOperation.TradeError	
InvalidParameter.RegexRuleError	
FailedOperation.MachineDelete	
LimitExceeded.AreaQuota	
InvalidParameter.ParsingError	
FailedOperation.RescanVul	
FailedOperation.Recover	
UnauthorizedOperation	
FailedOperation	
ResourceNotFound	
InvalidParameter.ReverShellKeyFieldAllEmpty	
FailedOperation.Export	
InvalidParameter.IllegalRequest	
InvalidParameter.MissingParameter	
FailedOperation.ProcessTaskNotFound	
AuthFailure	
InternalError	
FailedOperation.PrePayMode	